iConnectAccess624

Technical Reference / User Guide

Copyright

Copyright© 2006 OPEN Networks Pty Ltd. All rights reserved. The content of this manual is subject to change without notice. The information and messages contained herein are proprietary to OPEN Networks Pty Ltd. No part of this manual may be translated, transcribed, reproduced, in any form, or by any means without prior written permission by OPEN Networks Pty Ltd.

Disclaimer

For content and procedures available in this document, OPEN Networks Pty Ltd does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed.

Rev.: 2
Date Released: February 2006

Table Of Contents

Document Conventions **5**
Introduction **6**
System Requirements **7**
Host Operating Systems Support: 7
Web Browser Support: 7
Your iConnectAccess624 At A Glance **8**
Ports And Buttons 8
Reset 9
Front LED Panel 10
Installing Your iConnectAccess624 ..... **11**
Configuring Your Ethernet Network Card 11
For Windows® 98 Second Edition / Windows® Me 11
For Windows® 2000 / Windows® XP 12
Setting Up Your iConnectAccess624 ..... **13**
Default Settings 13
Log Into Your iConnectAccess624 14
Home Tab **15**
Setup Tab **16**
LAN Set Up 17
Accessing The LAN Configuration Screen 17
Enabling DHCP 18
Management IP 21
To Change The iConnectAccess624 IP Address: 21
Ethernet Switch 22
Wide Area Network (WAN) Setup 24
Connection Types 25
PPPoE Connection Type Set Up: 25
PPPoA Connection Type Set Up: 28
Bridged Connection Type Set Up: 31
Static Connection Type Set Up: 34
DHCP Connection Type Set Up: 37
Classical IP Over ATM (CLIP) Connection Set Up 40
Modify An Existing Connection 41
Modem Set Up 42
Advanced Tab **44**
UPnP 44
SNTP 46
SNMP 48
IP QoS 50
LAN Clients 54
Bridge Filters 55

Multicast 58
Static Routing 60
Dynamic Routing 62
Firewall 64
Port Forwarding 64
Custom Port Forwarding 67
Enable Incoming ICMP Ping 69
Access Control 69
DMZ Configuration 71
IP Filters 73
Tools 75
Remote Log 76
User Management 78
Update Gateway 80
Ping Test 81
Modem Test 82
Save / Restart Menu 84
Status 85
Network Statistics 86
Connection Status 87
DHCP Clients 88
Modem Status 89
Product Information 90
System Log 91
Index 92

Document Conventions

When using this manual, certain words are represented in different fonts, typefaces, and weights. This highlighting is systematic: different words are represented in the same style to indicate their inclusion in a specific category. The types of words represented in this way are listed in the following table:

Type Face	Used For:
Bold Typeface	■ GUI tabs; ■ GUI menu items; ■ Window and screen buttons
Italics	■ Window, dialog and screen names: ■ Titles; ■ Field names.
`User-entered data`	Data entered by the user
<Bold>	Computer keyboard commands

Also, different strategies are used to draw your attention to certain pieces of information. In order of how critical the information is to your system, these items are marked as Note, Tip or Warning. For example:

NOTE:

NOTE:

If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values.

TIP:

TIP:

Ensure your computer is configured for DHCP mode and that proxies are disabled in your browser.
You must also ensure that JavaScript support is enabled in browser settings, so that the browser does not display a login redirection screen. Finally, if any screen other than the Login screen appears, you may need to delete your temporary Internet files. (ie, basically flush the cached web pages).

WARNING:

WARNING!

If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values.

Introduction

Congratulations on the purchase of your iConnectAccess624. Fully-featured, it is the perfect high-speed ADSL Modem WAN bridge/router, specifically designed to connect your computer or LAN to the Internet and directly connect to your local area network via a high speed 10/100 Mbps Ethernet port.

The iConnectAccess624's extensive routing and bridging functions render it a flexible and scaleable platform for multiple users to access the Internet. Features include port forwarding and VPN pass-through, along with the ability to enable public or private Intranet solutions through a single IP address, using its RIP v 1 / 2 routing engine or NAPT features.

The highest levels of security are implemented in the iConnectAccess624, including Stateful Packet Inspection firewall and DMZ support for a full suite of security options against malicious intruders.

The iConnectAccess624 is fully compatible with all computers which support an Ethernet interface and are running a TCP/IP protocol stack. So, plug in the iConnectAccess624 (refer to the Quick Start Guide), configure it (per your ISP's instructions) and enjoy fast Internet access as never before!

System Requirements

A Pentium® MMX 233MHz or greater computer, installed with the following:

- CD-ROM drive;
- Ethernet card installed with TCP/IP Protocol (required only if you are connecting to the Ethernet port of your router);

Host Operating Systems Support:

- Windows® 98 Second Edition;
- Windows® 2000;
- Windows® Me;
- Windows® XP;
- OS independent for Ethernet.

Web Browser Support:

- Microsoft Internet Explorer 4.0 (or later versions);
- Netscape® Navigator 3.02 (or later versions).

Your iConnectAccess624 At A Glance

The iConnectAccess624 has different ports and LEDs. The following list details these:

Ports And Buttons

DSL

The phone cable connects from the ADSL port of the iConnectAccess624 to the ADSL port of your line filter. (ADSL Line)

RESET

This button resets your iConnectAccess624 to factory default settings. (All customized settings will be lost when you perform a reset.)

E1 – E4

The Ethernet cable connects from the Ethernet port/s of the iConnectAccess624 to the Ethernet LAN port of your computer.

DC 9V

The power cable connects from the DC port of the iConnectAccess624 to the mains power outlet. Remember to use only the power cable supplied with your iConnectAccess624, and ensure you switch the power switch to the ON position.

POWER

The power switch supplies power to the iConnectAccess624.

NOTE:

As each of the cables is connected, the corresponding LED will light up on the front of the iConnectAccess624.

Reset

Reset And Restore To Factory Defaults:

The Restore To Factory Defaults feature will reset the iConnectAccess624 to its factory default configuration. If configuration details in the router are changed, or following a firmware upgrade, you may lose the ability to configure it via the web interface. In order to restore this functionality, you may need to reset it to factory defaults.

To Reset The iConnectAccess624:

- Ensure that the iConnectAccess624 has been powered on for a minimum of 10 seconds.
- Use a blunt implement, such as a pencil or paperclip to press the reset button for 10 seconds, then release it.

NOTE:

During this time the reset is in progress. Do NOT power the iConnectAccess624 off whilst it resets.

The iConnectAccess624 will be reset to its factory defaults and once the indicator lights have returned to green (non-blinking), the reset is complete.

Front LED Panel

The following table displays the LED Status of each of the iConnectAccess624's LEDs and the definitions of each:

ADSL Front Panel LED	LED Status	Definition
POWER	Steadily Lit Up	Power is supplied to the iConnectAccess624.
	Flickering	N/A
E1 – E4	Steadily Lit Up	iConnectAccess624 Ethernet cable is properly connected to Computer Ethernet port.
	Flickering	Ethernet is transmitting / receiving data.
DSL	Steadily Lit Up	ADSL connection is established.
	Flickering	Router is trying to establish connection with ADSL Service Provider.
INTERNET	Steadily Lit Up	PPP connection to iConnectAccess624 is established.
	Flickering	N/A

Installing Your iConnectAccess624

step 1 Locate an optimum location for the iConnectAccess624.

step 2 Connect the Power Adaptor to mains power.

step 3 Now that the hardware installation is complete, you may need to configure Ethernet ports. Proceed to Configuring Your Ethernet Network Card for more information.

Configuring Your Ethernet Network Card

For Windows® 98 Second Edition / Windows® Me

NOTE:

Please note that these instructions may vary, depending on whether this is the first time you are configuring your Ethernet Driver in Windows. Those below are for first-time configurations.

step 1 From your Windows desktop, click *Start* > *Settings* > *Control Panel*.

step 2 From the *Control Panel* window, double-click the *Network* icon.

step 3 From the *Network* screen, highlight the *Configuration* tab to make it active.

step 4 From the *The following network components are installed* area of the window, select *TCP/IP-> xxx* where *xxx* refers to the model of the Ethernet card connected to your ADSL Router, click *Properties*.

step 5 From the *TCP/IP Properties* screen, click the *IP Address* tab to make it active.

step 6 Highlight the *Obtain an IP Address Automatically* radio button, and click **OK** to save the settings.

step 7 Ensure that the iConnectAccess624 is powered on. Restart your system when prompted.

For Windows® 2000 / Windows® XP

NOTE:

Please note that these instructions may vary, depending on whether this is the first time you are configuring your Ethernet Driver in Windows. Those below are for first-time configurations.

Windows® 2000:

step 1 From your Windows desktop, click *Start* > *Control Panel*.

step 2 From the *Control Panel* window, double-click the *Network Connections* icon.

step 3 At the *Network Connections* window, right-click on the *Local Area Connection* icon and click *Properties*.

step 4 Proceed from step 3 in the Windows XP Ethernet Driver Configuration Procedure below.

Windows® XP:

NOTE:

Instructions are based on the default Start *menu option.*

step 1 From your Windows desktop, click *Start* > *Control Panel*.

step 2 From the *Network Connections* window, right-click on the *Local Area Connection* icon and select **Properties**.

step 3 In the *Properties* window of the LAN connected, ensure that the *Connect Using* field indicates the model of the Ethernet Card connected to your iConnectAccess624.

NOTE:

This is important especially if you have more than one Local Area Connection icon displayed in the `Network Connections` *window. Ensure that you have selected the correct one.*

step 4 From the *This connection uses the following items:* area of the *Properties* window, select *Internet Protocol (TCP/IP)* and click **Properties**.

step 5 From the *General* tab of *Internet Protocol (TCP/IP) Properties* window, highlight the *Obtain an IP Address Automatically* radio button, and click **OK**.

step 6 Click **OK** again to close the dialog.

step 7 Ensure that your iConnectAccess624 is powered on. Restart your system when prompted.

Setting Up Your iConnectAccess624

This section will guide you through your iConnectAccess624's configuration via the web interface. The iConnectAccess624 is shipped with a standard PPP configuration.

Default Settings

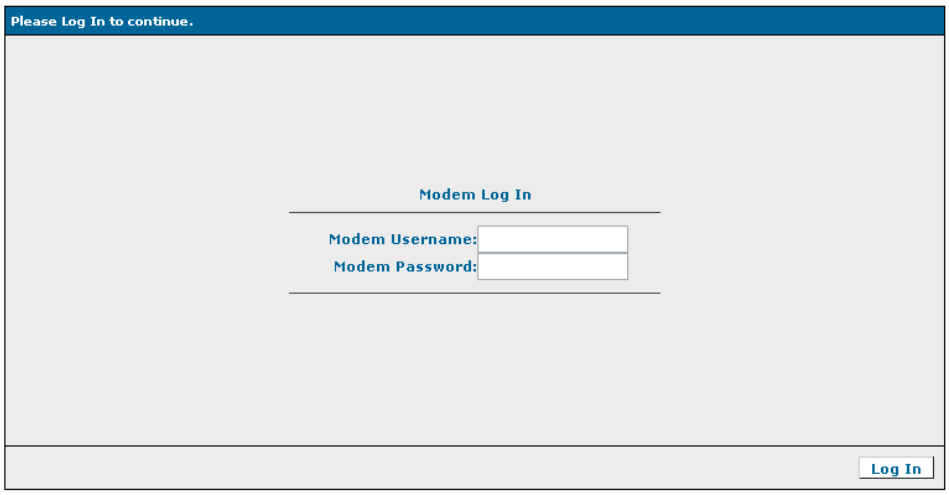
The following table lists the default settings for your iConnectAccess624. These settings may change depending on your DSL Provider / ISP. Please check with your DSL Provider / ISP for more information.

Setting	Default Value	
Login Username	root	
Login Password	ØP3N (0 = zero, P, 3, N)	
New Connection	*Name*	<blank>
	Username	<blank>
	Password	<blank>
	Protocol	PPPoE
	VPI	8
	VCI	35
	Authentication	Auto
LAN Configuration	*IP Address*	192.168.1.254
	Netmask	255.255.255.0
	Server On Enabled	
	Start IP	192.168.1.100
	End IP	192.168.1.200
	Lease Time	604800 sec (7 days)

Log Into Your iConnectAccess624

To Configure Your iConnectAccess624:

step 1 Open your web browser and enter `http://192.168.1.254` in the *Address* bar, then click **<Enter>**. The following appears:



step 2 In the *Log In* screen, enter `root` (case sensitive) in the *Username* field and in the *Password* field, enter `ØP3N` (0 = zero, P, 3, N - case sensitive).

step 3 Click **Log In**.

TIP:

Ensure your computer is configured for DHCP mode and that proxies are disabled in your browser. See the procedures on configuring your Ethernet. You must also ensure that JavaScript support is enabled in browser settings, so that the browser does not display a login redirection screen. Finally, if any screen other than the Login screen appears, you may need to delete your temporary Internet files. (ie, basically flush the cached web pages).

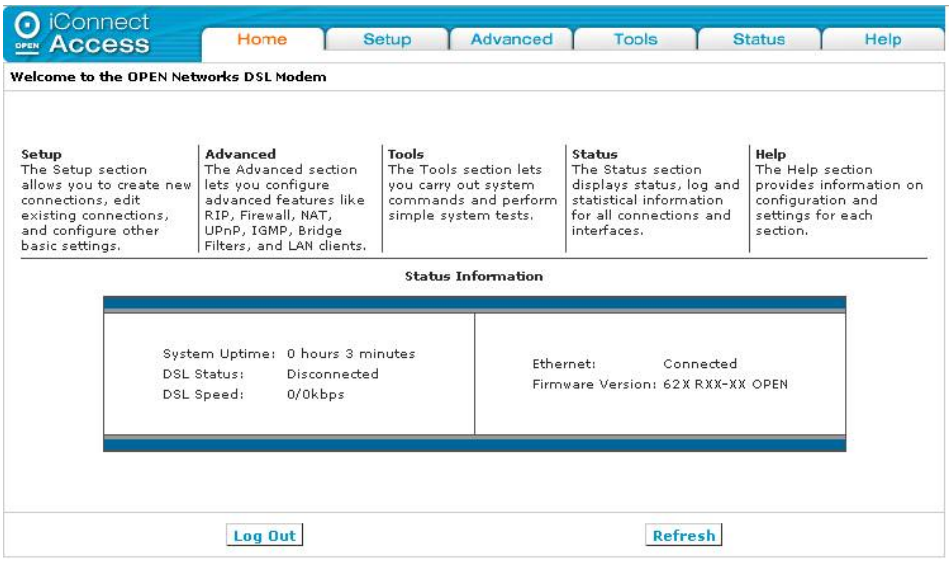
Logging in allows you to access the iConnectAccess624's web interface. This consists of the following six tabs that provide all the options you need to configure your iConnectAccess624:

Tab	Function
Home	Screen listing all available modem web interface configuration options, and modem status information.
Setup	Configuration of LAN and WAN Settings
Advanced	Configuration of advanced options within the iConnectAccess624 such as security, routing and filtering.
Tools	Access tools and diagnostics to assist in debugging.
Status	Obtain the status of the iConnectAccess624.
Help	View the online help.

Home Tab

After you have logged in, the first screen to appear will be the **Home** tab screen. This is the screen from which you navigate to all other modem configuration options, by clicking the appropriate tab.

It also displays the status and details of your connection, including the DSL speed and the firmware version. You can click the **Refresh** button to update the system status details as required.


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Welcome to the OPEN Networks DSL Modem
Setup
The Setup section allows you to create new connections, edit existing connections, and configure other basic settings.
Advanced
The Advanced section lets you configure advanced features like RIP, Firewall, NAT, UPnP, IGMP, Bridge Filters, and LAN clients.
Tools
The Tools section lets you carry out system commands and perform simple system tests.
Status
The Status section displays status, log and statistical information for all connections and interfaces.
Help
The Help section provides information on configuration and settings for each section.
Status Information
System Uptime: 0 hours 3 minutes
DSL Status: Disconnected
DSL Speed: 0/0kbps
Ethernet: Connected
Firmware Version: 62X RXX-XX OPEN
Log Out
Refresh

Setup Tab

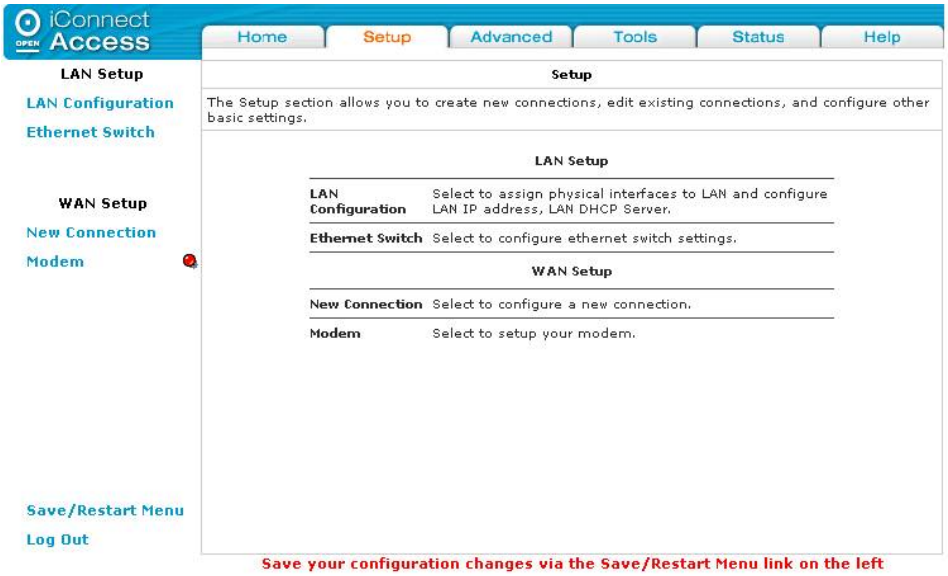
The *Setup* tab allows you to set up the LAN and WAN sides of your networks, including:

- DHCP Configuration;
- Management IP;
- New WAN Connections;
- Modem Configuration.

Accessing The Setup Main Screen:

From any screen of the web interface,

- Click **Setup**. The following screen appears:



The *Setup* screen consists of two set up subsections: *LAN Setup* and *WAN Setup*. From here you can select the LAN and WAN Settings you wish to configure by clicking the appropriate links from the menu list.

LAN Set Up

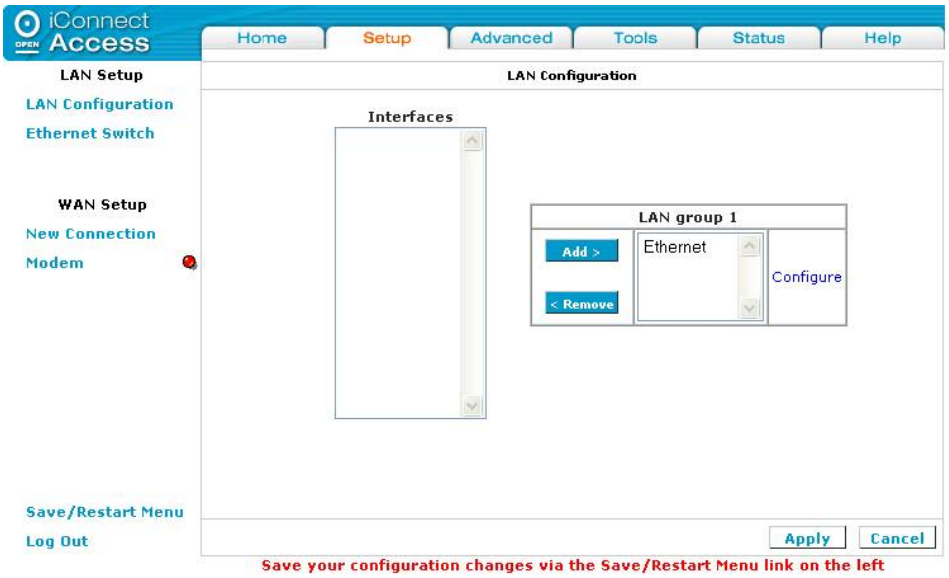
By default, your iConnectAccess624 has the DHCP server (LAN side) enabled. If you already have a DHCP server running on your network, you must disable one of them; if you connect a second DHCP server into the network, you will experience network errors and the network will not function normally.

Accessing The LAN Configuration Screen

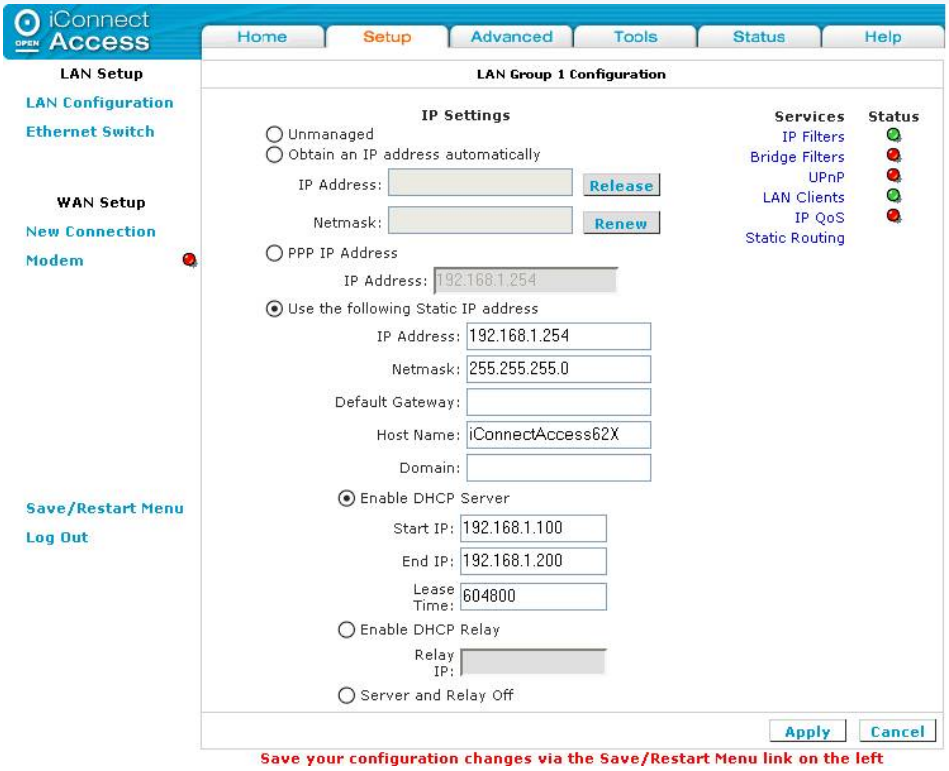
Before configuring the IP settings for your LAN, you will need to select the Ethernet interface type to set up in the *LAN Configuration* screen.

To do this, from any web interface screen:

step 1 Click **Setup**, then **LAN Configuration**. The following screen appears:



step 2 From the *LAN group 1* area of the screen, highlight *Ethernet*, then click **Configure**. The following screen appears.



Enabling DHCP

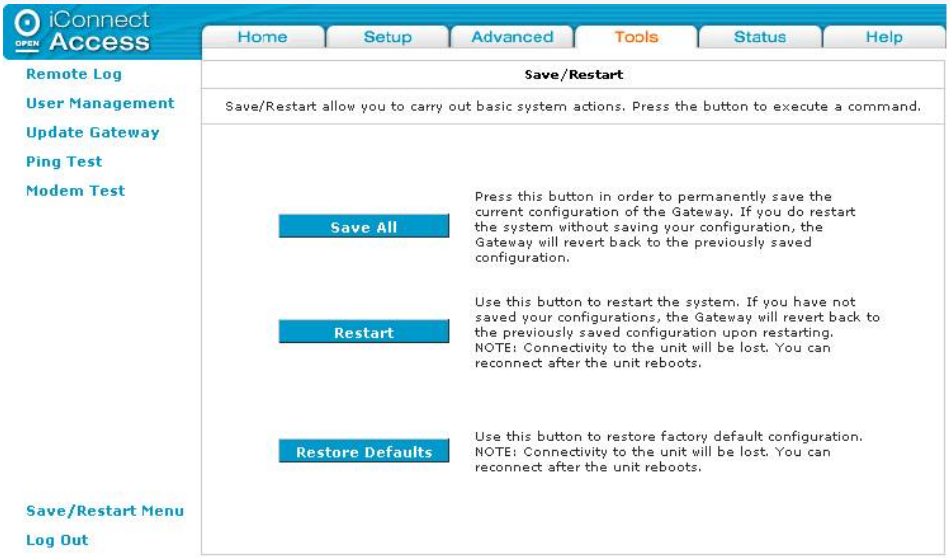
step 1 Follow steps 1 to 2 of the *Accessing The LAN Configuration Screen* procedure.

step 2 In the *Enable DHCP Server* area of the screen, highlight the *Enable DHCP Server* radio button.

step 3 Enter the Start IP Address in the *Start IP:* field. This address is the beginning of the range from which the DHCP Server starts issuing IP addresses.

step 4 Enter the End IP Address in the *End IP Address* field. This address is the end of the range from which the DHCP Server issues IP addresses.

step 5 Click **Apply,** then click the **Save / Restart Menu** link. The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 6 Click **Save All** to save the changes permanently.

The following table lists the *LAN Group 1 Configuration* screen fields and their definitions:

Field	Description
Unmanaged	Highlight this radio button if this interface does not require a management IP address.
Obtain an IP address automatically	Check this checkbox if the 624 is acting as a DHCP client. The 624 will receive an IP Address from the specified DHCP server.
IP Address	This field will be populated when the iConnectAccess624 receives an IP Address from a DHCP Server.
Netmask	This field will be populated when the iConnectAccess624 receives an IP Address from a DHCP Server.
Use the following Static IP Address	Highlight this radio button to use a static address for your router.
IP Address	The *Default IP Address* for the iConnectAccess624 is `192.168.1.254`. Its *Subnet Mask* is `255.255.255.0`, and this allows you to support 254 users. If you wish to support a larger number of users, you can alter the Subnet Mask. However, if you do, remember the DHCP Server is defaulted to give out 101 IP Addresses.
Netmask	A mask used to determine the subnet to which an IP address belongs. This is the Subnet Mask that will be assigned to the Management interface of the iConnectAccess624.
Default Gateway	The default gateway is a host to which local computers send data that is destined for a non-local machine. On the iConnectAccess624, configure the default gateway address here to reach all computers that are not on the same local IP subnet. This is usually delivered automatically by the ISP.
Hostname	This is the assigned hostname for the iConnectAccess624. The *Hostname* can be any alphanumeric word that does not contain spaces.
Domain	The *Domain Name* is used in conjunction with the *Hostname* to uniquely identify the iConnectAccess624. Domain Names always have 2 or more parts, separated by dots. The part on the left is the most specific, and the part on the right is the most general. Usually, all of the hosts on a given Network will have the same part as the right-hand portion of their Domain Names.
Enable DHCP Server	Highlighting the *Enable DHCP Server* radio button turns on the DHCP server. This will need to be disabled if a DHCP server is already running on the LAN. The DHCP Server is set to on by default.
Start IP	This address is the beginning of the range from which the DHCP Server starts issuing IP addresses. You need to ensure the

Field	Description
	iConnectAccess624 Management IP address and any statically-defined addresses are not within the DHCP start and end address ranges. The default Start IP address is `192.168.1.100`.
End IP	This is the end of the DHCP Server IP address range. The default End IP is `192.168.1.200`.
Lease Time	The *Lease Time* is the amount of time a LAN computer will hold the IP address. The IP Address will automatically renew after this time has elapsed. If the LAN computer does not renew the address after the lease period the lease information will be removed from the DHCP database. This database can be viewed under **Tools> DHCP Clients**. The lease time is in units of seconds; the default value is `604800` seconds (7 days).
Enable DHCP Relay	Highlighting the *Enable DHCP Relay* radio button configures the iConnectAccess624 to forward the DHCP request to a remote DHCP server. Enter the remote DHCP server address in the *Relay IP* field.
Server and Relay Off	This will disable the iConnectAccess624's DHCP server and relay functionality.
Services	Click the appropriate link to move quickly to the services you wish to configure for the interface type.
Status	The green radio buttons indicate the services which are running by default for the interface you are configuring.

Management IP

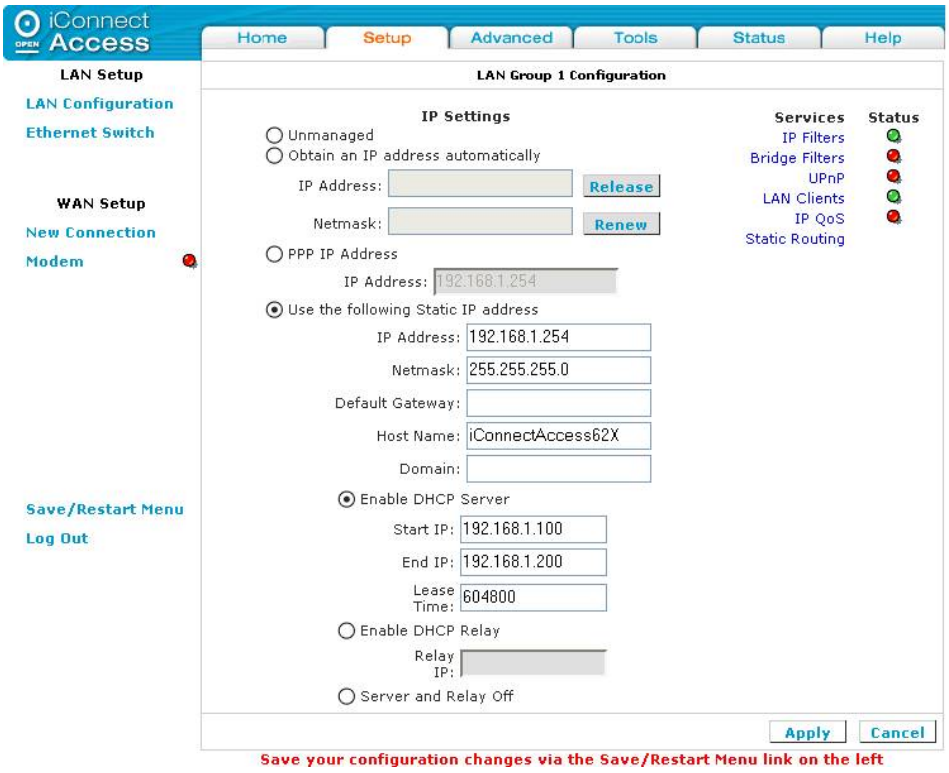
The Management IP area of the web interface allows you to configure the LAN IP Address details for the iConnectAccess624.

NOTE:

If you change this address from the default, you will need to reconnect using your new IP Address.

To Change The iConnectAccess624 IP Address:

step 1 Follow steps 1 to 2 of the *Accessing The LAN Configuration Screen* procedure. The following appears:



step 2 Ensure the *Use the following Static IP address* radio button is highlighted, and in the area beneath the *Use the following Static IP address* field, enter the IP Address in the *IP Address* field as required.

step 3 Enter the netmask in the *Netmask* field as required.

step 4 Enter the default gateway as provided by your DSL Provider / ISP in the *Default Gateway* field. This is optional.

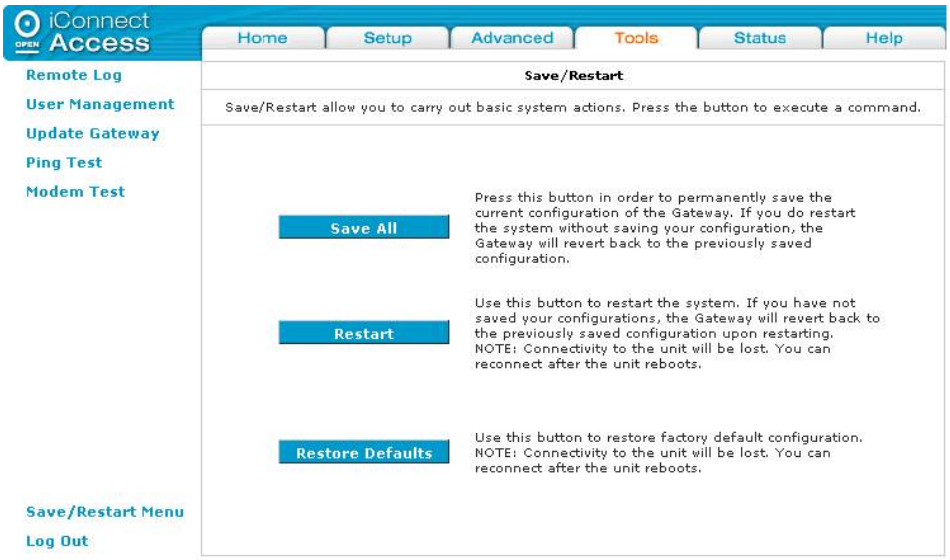
step 5 Enter an alphanumeric Hostname in the *Hostname* field. This cannot contain spaces.

step 6 Enter the Domain Name in the *Domain Name* field. This cannot contain spaces.

NOTE:

The Domain Name *is used in conjunction with the Hostname to identify the iConnectAccess624 uniquely. To access the iConnectAccess624's web pages you can type the IP* `192.168.1.254` *or* `mygateway.ar7` *in the web browser. Using the Hostname in the browser requires the workstation to have its DNS server set to the iConnectAccess624.*

step 7 Click **Apply,** then click the **Save / Restart Menu** link**.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 8 Click **Save All** to save the changes permanently.

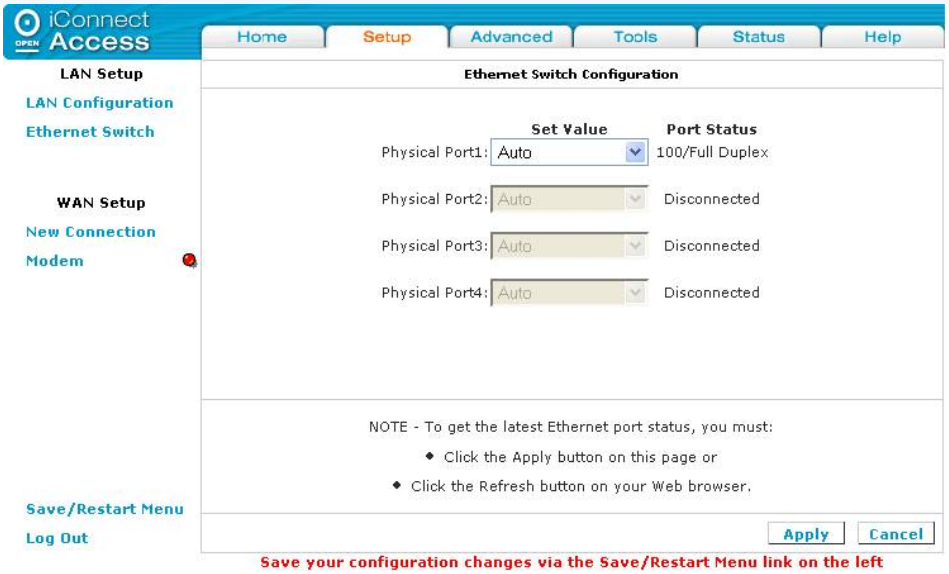
Ethernet Switch

This screen is used to hard set the Ethernet Speed and duplexing options. It is recommended that that all ports be set to auto.

To Modify the Ethernet Switch Configuration:

From any screen in the web interface,

step 1 Click the **Setup** tab, then **Ethernet Switch** from the *LAN Setup* menu. The following screen appears:



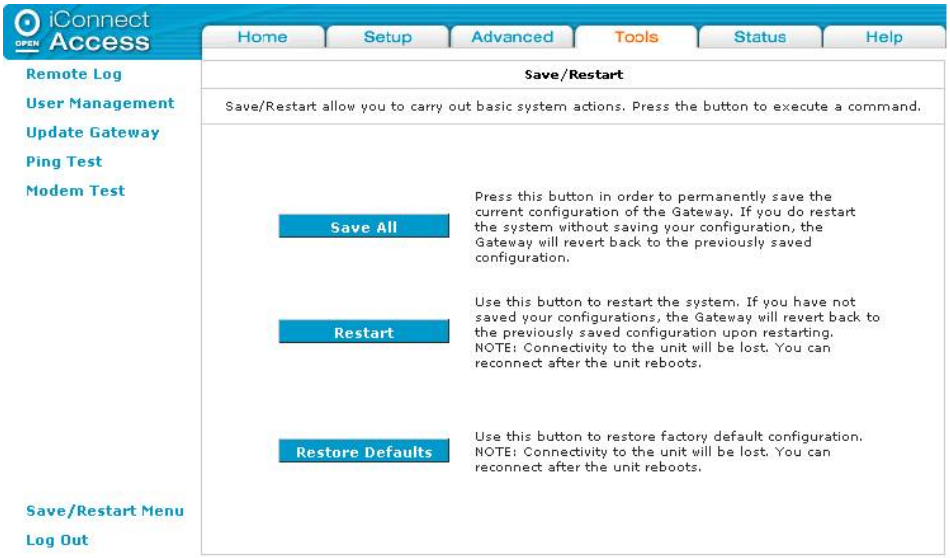
step 2 From the *Physical Port1* drop-down list, select the ethernet port for which you wish to change the hardware setting. The options are: *Auto, 10\Half Duplex, 10\Full Duplex, 100\Half Duplex* and *100\Full Duplex*.

step 3 Edit each Ethernet port as required.

NOTE:

The Fallback column in this screen displays the speed and duplexing (the mode of carrying data in two directions) that has been negotiated on the port.

step 4 Click **Apply**, then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart Menu
Log Out
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

step 5 Click **Save All** to save the changes permanently.

Wide Area Network (WAN) Setup

Before the router will pass any data between the LAN and WAN interfaces, the WAN side of the iConnectAccess624 must be configured. Depending on your DSL service provider or ISP, you will need some (or all) of the information outlined below before you can properly configure the WAN. The following table lists all DSL requirements:

DSL Requirement	Comment
Line	
VPI and VCI	The VPI (Virtual Path Identifier) and the VCI (Virtual Channel Identifier) define the virtual path settings for the ADSL connection between you and your ISP. By default, these settings are pre-configured for 8/35 in your iConnectAccess624. If you wish to change them, please ensure you obtain the correct VPI/VCI setting details form your ISP.
Encapsulation and Multiplexing	For PPPoA, Static, Bridge, DHCP and CLIP authentication types, you may have to define the encapsulation parameters. The iConnectAccess624 has two options for encapsulation: LLC encapsulation and VCMux. The default encapsulation type for the iConnectAccess624 is LLC. If you wish to change these settings, please ensure you obtain the correct encapsulation setting details form your ISP.
Training Mode	The default is MMODE, and this enables your iConnectAccess624 to tune into the ADSL services in Australia automatically. Do not change this parameter.
PPPoA / PPPoE Requirement	
Username	Your username is required for authentication for your Internet service.
Password	Your username is required for authentication for your Internet service.
Static Type Requirement	
DSL Fixed Internet IP Address	
Subnet Mask	
Default Gateway	
Primary DNS IP Address	

The iConnectAccess624 supports the following connection types:

- PPPoE
- PPPoA
- Bridged;
- Static;
- DHCP;
- CLIP.

Connection Types

Your iConnectAccess624 can support up to eight unique virtual connections to different destinations, all using the same bandwidth simultaneously. If you have multiple virtual connections, you may need to utilize the static and dynamic routing capabilities of the router to pass data correctly.

PPPoE Connection Type Set Up:

Computers connected to the Internet via ADSL do so through an Ethernet link. As such, plain TCP/IP has been used, with no additional protocols. PPP (Point-to-Point Protocol) provides secure login, and traffic metering among other advanced features. PPPoE (PPP over Ethernet) was designed to bring the security and metering benefits of PPP to Ethernet connections such as DSL.

PPPoE allows ADSL users to be authenticated by the ISP's Radius authentication systems. Most broadband connections are Ethernet, hence Point-to-Point Protocol over Ethernet. It also allows for ISPs to provide multiple services over multiple PPP sessions, ie, rated services, broadband specific content (movies, etc.), metered services, etc.

To Configure PPPoE:

From any screen in the web interface,

step 1 Click **Setup**.

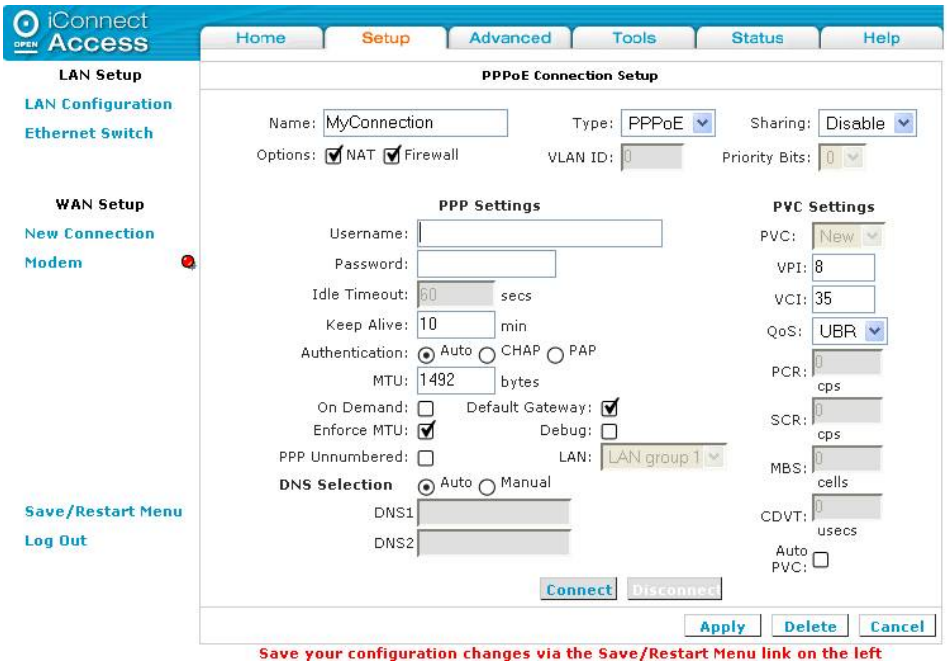
step 2 From the *WAN Setup* menu, click **New Connection**.
The default *PPPoE Connection Setup* screen appears.

NOTE:

If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values.

---

step 3 From the *Type* drop-down list, select *PPPoE*. The following is displayed:



step 4 Enter a unique name for your PPPoE connection in the *Name* field. The name must not have spaces and cannot begin with numbers.

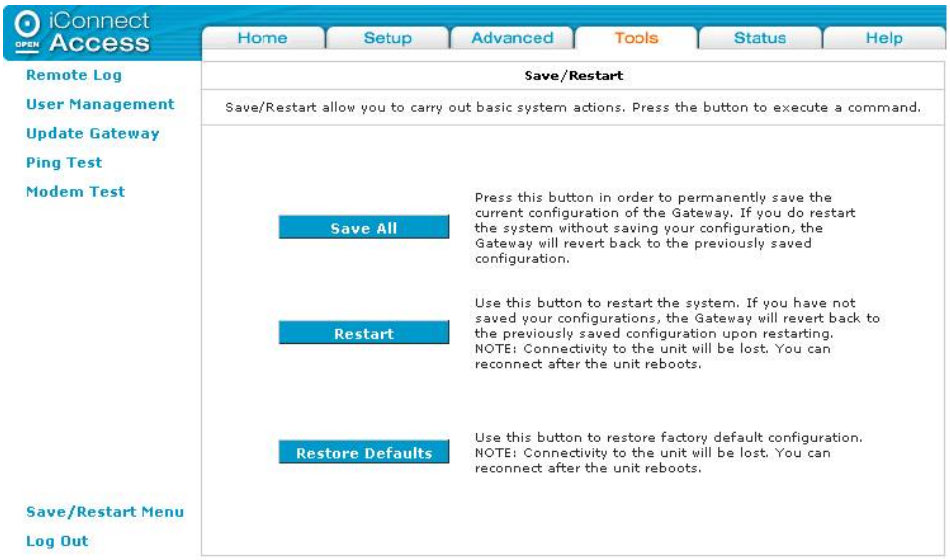
step 5 Check the *NAT* and *Firewall* checkboxes beside the *Options* field.

step 6 Enter your DSL Provider / ISP username and password in the *Username* and *Password* fields.

step 7 Enter the DSL Provider / ISP-provided *VPI* and *VCI* settings.

step 8 Click **Connect.**

step 9 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 10 Click **Save All** to save the changes permanently.

The following table lists the *PPPoE Connection* type fields and describes each of the options:

Field	Description
NAT	Network Address Translation is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.
Firewall (SPI)	Check this checkbox to monitor traffic passing between your LAN and the outside world on this connection, to prevent security breaches. This is set to *Enabled* by default for standard operation.
Username	The Username for your ISP account.
Password	The Password for your ISP account.
On-Demand	If selected, this enables on-demand connectivity to the Internet. Connection is activated when traffic from the LAN is generated. This is unchecked by default.
Idle Timeout	This specifies that the PPPoE connection should disconnect if the link detects no activity for x seconds. If you wish to ensure the link remains always connected, enter `0` in this field. This option will only be available when the *On-Demand* option is checked.
Keep Alive	When the *On-Demand* option is disabled, this value specifies the time to wait without connection to your provider before terminating the connection. If you wish to ensure the link remains always active, enter `0` in this field. This is set to `0` by default.
Authentication	This defines the authentication protocol for your ISP. This is set to *Auto* by default.
MTU	Enter the *Maximum Transmission Unit* for the DSL connection. The default value is set to `1492`.
VPI	The *VPI (Virtual Path Identifier)* defines the virtual path settings for the ADSL connection between you and your ISP. The value entered here must be supported by your ISP.
VCI	The *VCI (Virtual Channel Identifier)* defines the virtual channel settings for the ADSL connection between you and your ISP. The VCI value entered here must be supported by your ISP.
QoS	QoS defines the iConnectAccess624 capabilities that provide guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities. Three different Quality Of Service options are available in the iConnectAccess624: UBR, CBR and VBR. The QoS selected here must be supported by your ISP. By default this is set to *UBR*.
LAN	Select the LAN Group (as defined in the *LAN Configuration* screen) of which the PPPoE connection will be part.
Default Gateway	Check this checkbox to set this connection as the default gateway in the routing table.
Debug	Check this checkbox to enable PPP connection debugging facilities.
Connect	Click the **Connect** button to use the current settings to establish a PPP connection. Note that in *On Demand* mode the Connect button is disabled.
Disconnect	Click the **Disconnect** button to disconnect the PPP connection.

PPPoA Connection Type Set Up:

PPPOA or PPPoA, Point-to-Point Protocol (PPP) over ATM, is a network protocol for encapsulating PPP frames in ATM AAL5. It used mainly with ADSL services and is compliant with RFC 2364. PPP over ATM adaptation layer 5 (AAL5) – PPPoA uses AAL5 as the framed protocol, which supports both PVC and SVC.

PPPoA was primarily implemented to support PPP sessions over the ADSL network. It relies on RFC1483, operating in either Logical Link Control-Subnetwork Access Protocol (LLC-SNAP) or VC-Mux mode. A Customer Premises Equipment (CPE) device, normally an ADSL modem, encapsulates the PPP sessions for transport across the ADSL network and the Digital Subscriber Line Access Multiplexer (DSLAM).

It offers standard PPP features such as authentication, encryption, and compression.

To Configure The iConnectAccess624 For PPPoA:

From any screen in the web interface,

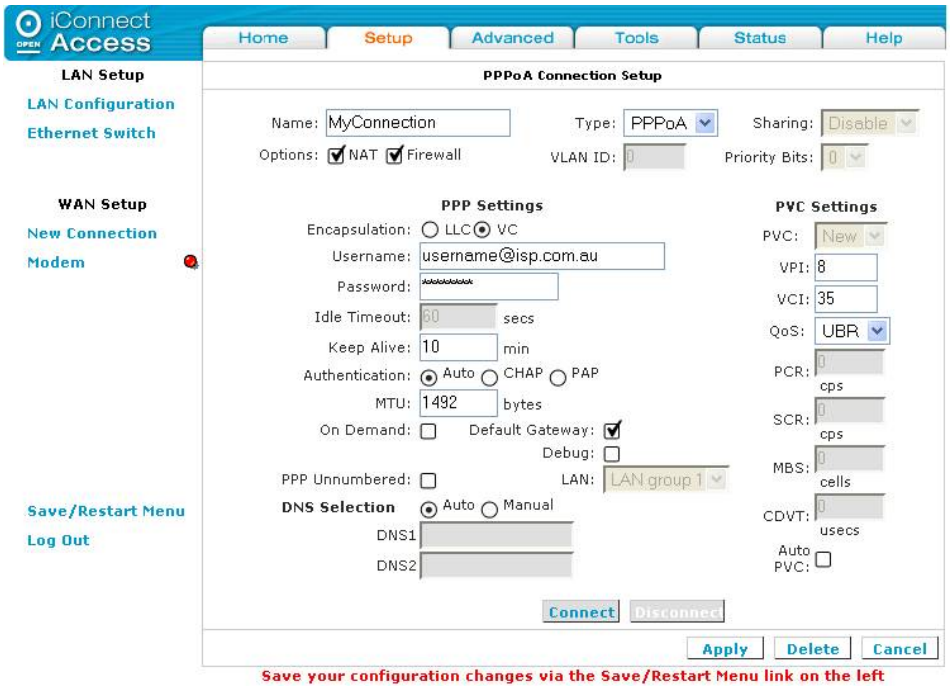
step 1 Click **Setup**.

step 2 Under the *WAN Setup* menu, click **New Connection**.
The default PPPoE Connection type screen appears.

NOTE:

If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values.

step 3 From the *Type* drop-down list select *PPPoA*. The following appears:



step 4 Check the *NAT* and *Firewall* checkboxes beside the *Options* field.

step 5 Enter a unique name for the PPPoA connection in the *Name* field. The name must not have spaces and cannot begin with numbers.

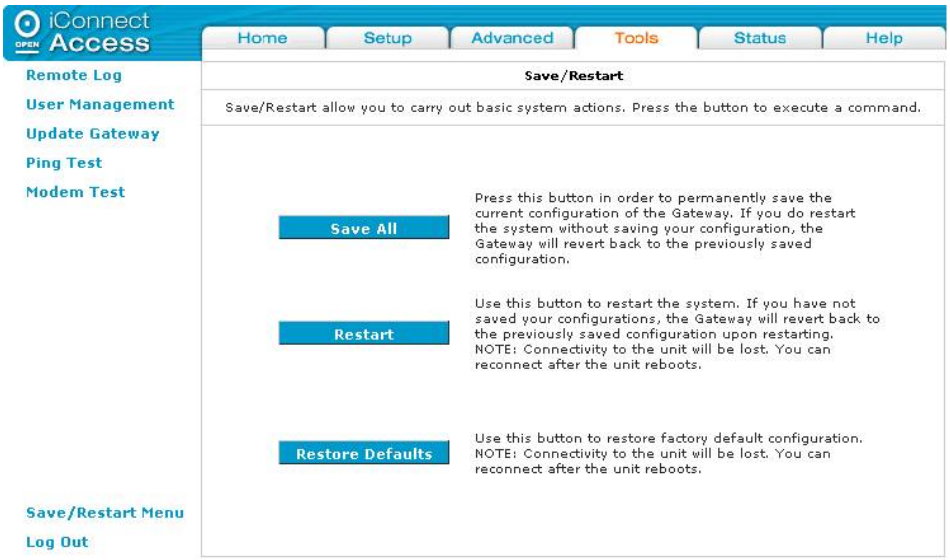
step 6 Select the encapsulation type (*LLC* or *VC*) by highlighting the appropriate radio button. If you are not sure leave this set to the default.

step 7 Enter your DSL Provider / ISP username and password in the *Username* and *Password* fields.

step 8 Enter the *VPI* and *VCI* settings as supplied by your DSL service provider / ISP.

step 9 Click **Connect.**

step 10 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 11 Click **Save All** to save the changes permanently.

The following table lists the *PPPoA Connection Set Up* screen fields and describes each of the options:

Field	Description	
NAT	Network Address Translation is a feature that enables you to use private IP addresses on your computer or LAN. This is set to *Enabled* by default for standard operation.	
Firewall	Check this checkbox to monitor traffic passing between your LAN and the outside world on this connection, to prevent security breaches. This is set to *Enabled* by default for standard operation.	
Encapsulation	LLC and VC are two different methods of encapsulating multiple sessions. This is set to *LLC* by default.	
	LLC	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
	VC	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol
Username	The username for your ISP account.	
Password	The password for your ISP account.	
On-Demand	If selected, this enables on-demand connectivity to the Internet. Connection is activated when traffic from the LAN is generated. This is unchecked by default.	
Idle Timeout	This specifies that the PPPoE connection should disconnect if the link detects no activity for x seconds. If you wish to ensure the link remains always connected, enter 0 in this field. This option will only be available when the *On-Demand* option is checked.	
Keep Alive	When the *On-Demand* option is disabled, this value specifies the time to wait without connection to your provider before terminating the connection. If you wish to ensure the link remains always active, enter 0 in this field. This is set to 0 by default.	

Field	Description
MTU	Enter the *Maximum Transmission Unit* for the DSL connection. The default value is set to `1500`.
VPI	The *VPI (Virtual Path Identifier)* defines the virtual path settings for the ADSL connection between you and your ISP. The VPI value entered here must be supported by your ISP.
VCI	The *VCI (Virtual Channel Identifier)* defines the virtual channel settings for the ADSL connection between you and your ISP. The VCI value entered here must be supported by your ISP.
QoS	QoS defines iConnectAccess624 capabilities that provide guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities. Three different Quality Of Service options are available in the iConnectAccess624. These are UBR, CBR and VBR. The QoS selected here must be supported by your ISP. By default this is set to *UBR*.
Default Gateway	Check this checkbox to set this connection as the default gateway in the routing table.
Debug	Check this checkbox to enable PPP connection debugging facilities.
Connect	Click the **Connect** button to use the current settings to establish a PPP connection. Note that in *On Demand* mode the Connect button is disabled.
Disconnect	Click the **Disconnect** button to disconnect the PPP connection.

Bridged Connection Type Set Up:

In Bridged mode, Ethernet frames are bridged over ATM Virtual Circuits. The Ethernet frames are encapsulated using either LLC Encapsulation or VC Multiplexing. Since the Ethernet packets are bridged, the router's only functionality is to pass the Ethernet packets to and from the Internet Service Provider and the local network. The IP addresses of the local network are assigned by the ISP either statically or dynamically.

In this setting, NAT and firewall rules are disabled. This connection method makes the iConnectAccess624 act as a transparent hub, and passes packets across from the WAN interface to the LAN interface transparently.

If your ISP provides a bridged service, this is the type that you should select.

To Configure The iConnectAccess624 As A Bridge:

From any screen in the web interface,

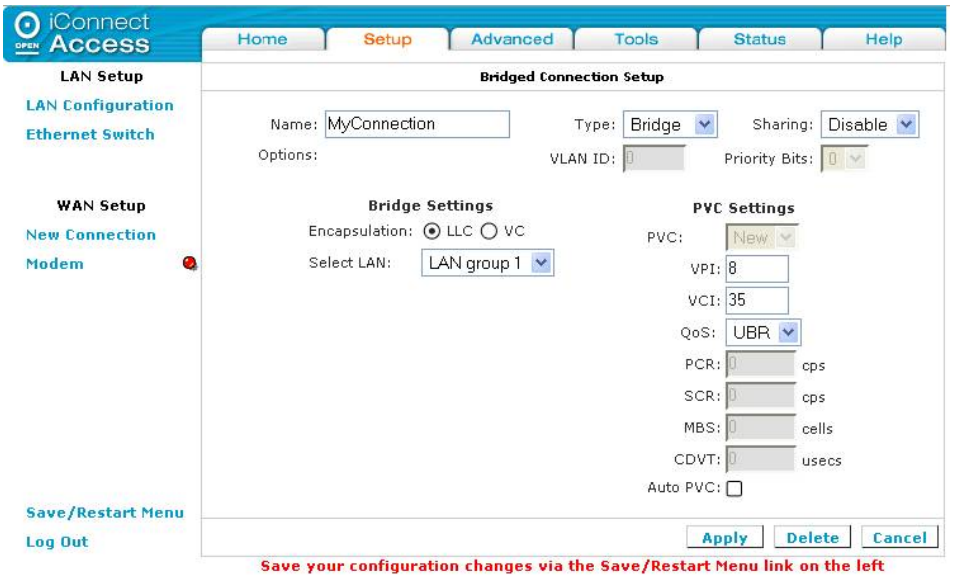
step 1 Click the **Setup** tab.

step 2 Under the *WAN Setup* menu item, click **New Connection**. The default PPPoE connection set up is displayed.

NOTE:

If you need to use the VPI and VCI values in an existing connection, you will need to open the connection and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values unless sharing is enabled.

step 3 From the *Type* drop-down list, select *Bridge*. The following screen appears:



step 4 Enter a unique name for the connection type in the *Name* field.

NOTE:

The **Name** *must not contain spaces or begin with numbers.*

step 5 Highlight either the *LLC* or *VC* radio button, depending on the encapsulation type for your configuration. If you are not sure, leave this as the default.

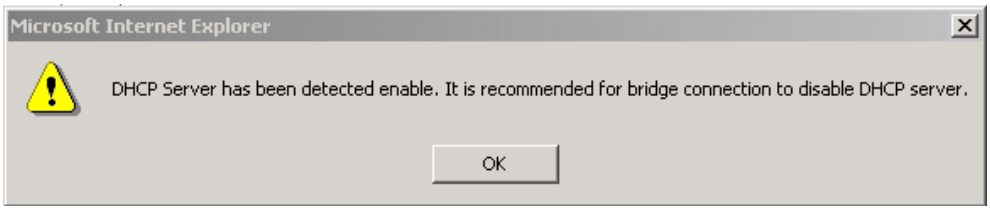
step 6 Enter the *VPI* and *VCI* settings as supplied to you by your DSL Provider / ISP.

step 7 From the *QoS* drop-down list, select the quality of service. Leave the default value if you are unsure of this.

step 8 Click **Apply.**

NOTE:

*If you have added a Bridged connection and need to edit it, once you make a change and click the **Apply** button, and DHCP is enabled, the following warning message may appear.*

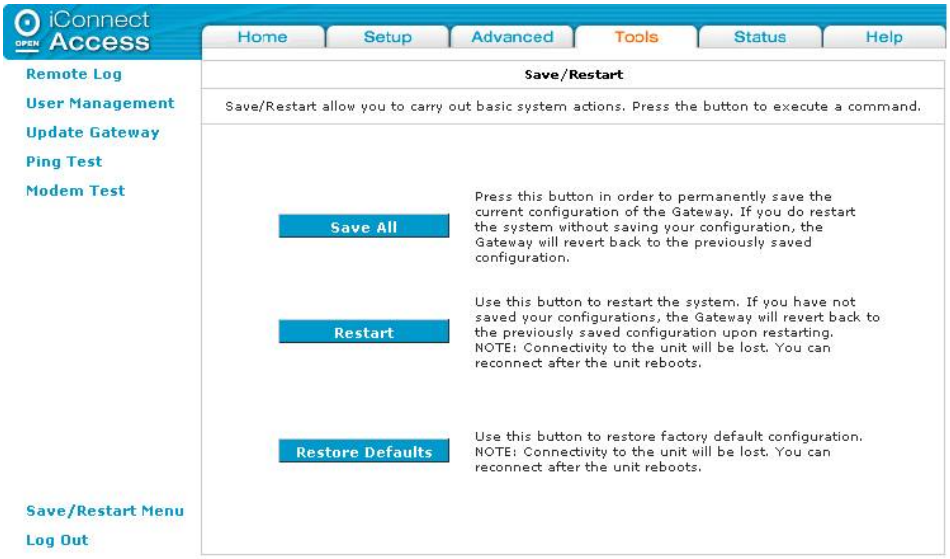

Microsoft Internet Explorer
DHCP Server has been detected enable. It is recommended for bridge connection to disable DHCP server.
OK

step 9 Click **OK** and follow the instructions below to disable the DHCP server.

NOTE:

*To disable the DHCP Server you will need to access the LAN Set Up procedure in this Technical Reference. Once you reach the LAN Group 1 screen, highlight the name of the Bridged connection, then highlight the Server and Relay Off radio button, and click **Apply.** You will then need to complete steps 10 and 11 below.*

step 10 From the *Bridged Connection Setup* screen, click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 11 Click **Save All** to save the changes permanently.

The following table lists the *Bridged Connection Setup* screen fields and their definitions:

Field	Description	
Encapsulation	LLC and VC are two different methods of encapsulating multiple sessions. This is set to *LLC* by default.	
	LLC	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
	VC	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
VPI	The VPI (Virtual Path Identifier) defines the virtual path settings for the ADSL connection between you and your ISP. The VPI value entered here must be supported by your ISP.	
VCI	The VCI (Virtual Channel Identifier) defines the virtual channel settings for the ADSL connection between you and your ISP. The VCI value entered here must be supported by your ISP.	
QoS	QoS defines iConnectAccess624 capabilities that provide guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities. There are three different quality of service options available in the iConnectAccess624. These are UBR, CBR and VBR. The QoS selected here must be supported by your ISP. By default this is set to *UBR*.	

Static Connection Type Set Up:

A Static Connection type is used whenever a known static IP address is assigned. The accompanying information such as the Subnet Mask and the Gateway should also be specified. Up to three Domain Name Server (DNS) addresses can also be specified. These servers would enable you to have access to other web servers. The valid IP Address range is from 0.0.0.0 to 255.255.255.255.

Static Connection Configuration:

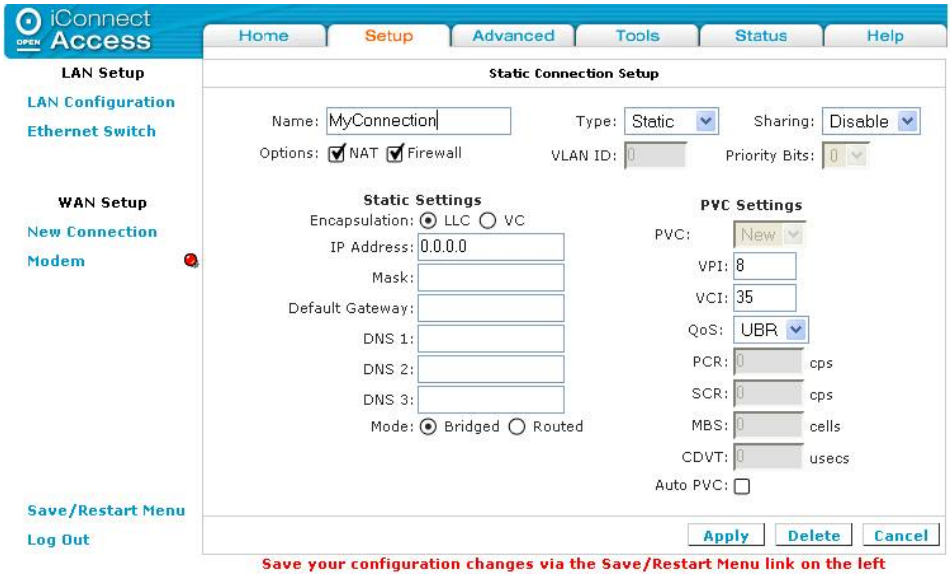
From any screen in the web interface,

step 1 Click **Setup** , then click **New Connection** from the *WAN Setup* menu. The default *PPPoE Connection Setup* screen appears.

step 2 From the *Type* drop-down list, select *Static*. The following appears:

NOTE:

If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values.



step 3 Enter a unique name for your static connection in the *Name* field. The name must not have spaces and cannot begin with numbers.

step 4 You can also enable *Network Address Translation (NAT)* and the *Firewall* options. If you are unsure, leave these in the default mode.

step 5 Select the encapsulation type (*LLC* or *VC*) by highlighting the appropriate radio button. If you are unsure leave the setting as default.

step 6 Enter the *VPI* and *VCI* settings as provided by DSL service provider / ISP.

step 7 In the *IP Address* field, enter your assigned IP address based on the information provided by your DSL Provider / ISP.

step 8 In the *Mask* field enter the Subnet Mask based on the details provided by your DSL Provider / ISP.

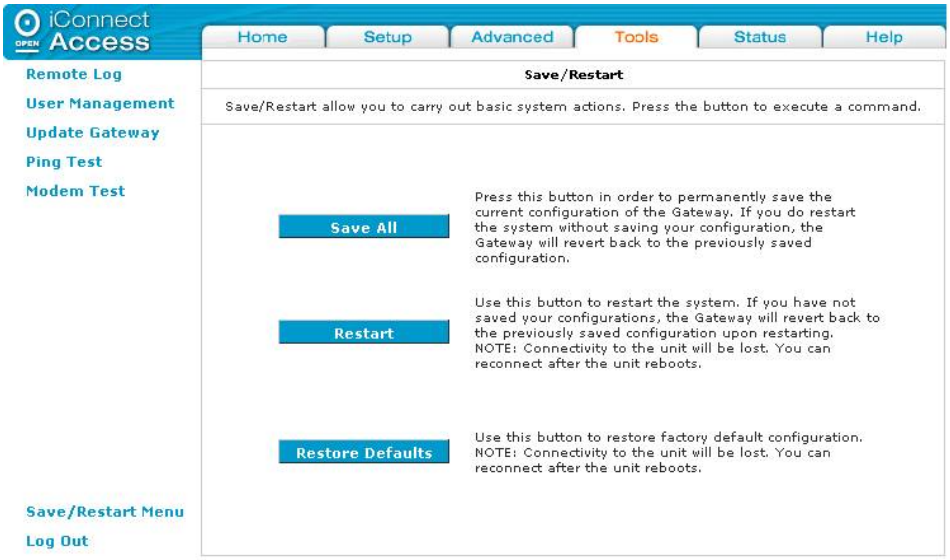
step 9 In the *Default Gateway* field enter the Default Gateway based on the information provided by your DSL Provider / ISP (if provided).

step 10 In the *DNS 1* and *2* fields, enter the *Domain Name Services (DNS)* values based on the information provided by your DSL Provider / ISP (if provided).

step 11 In the *Mode* field, highlight the required connection type radio button as

appropriate. The options are *Bridged* and *Routed*.

step 12 Click the **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 13 Click **Save All** to save the changes permanently.

The following table lists the *Static Connection Setup* screen fields and their definitions:

Field	Description	
NAT	Network Address Translation is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.	
Firewall (SPI)	Check this checkbox to monitor traffic passing between your LAN and the outside world on this connection, to prevent security breaches. This is set to *Enabled* by default for standard operation.	
Encapsulation	LLC and VC are two different methods of encapsulating multiple sessions. This is set to *LLC* by default.	
	LLC	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
	VC	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol
IP Address	This is the static IP that will be assigned to the WAN interface of the iConnectAccess624. This will be provided by your ISP.	
Mask	A mask used to determine to which the subnet an IP address belongs. This is the Subnet Mask that will be assigned to the WAN interface of the iConnectAccess624. This will be provided by your ISP.	
Default Gateway	The default gateway is a host to which local computers send data that is destined for a non-local machine. On the iConnectAccess624, configure the default gateway address here to reach all computers that are not on the same local IP subnet.	
DNS 1 – DNS 3	DNS service is used to translate a Domain Name into a corresponding IP address. The DNS server name should be obtained from your ISP.	
Mode	*Routed* or *Bridged* mode can be selected here.	
PVC	*Select a PVC from the drop-down list.*	
VPI	The *VPI (Virtual Path Identifier)* defines the virtual path settings for the ADSL connection between you and your ISP. The VPI value entered here must be supported by your ISP.	
VCI	The *VCI (Virtual Channel Identifier)* defines the virtual channel settings for	

Field	Description
	the ADSL connection between you and your ISP. The VCI value entered here must be supported by your ISP.
QoS	QoS defines the iConnectAccess624 capabilities that provide guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities. Three different quality of service options are available in the iConnectAccess624. These are UBR, CBR and VBR. The QoS selected here must be supported by your ISP. By default this is set to *UBR*.

DHCP Connection Type Set Up:

Dynamic Host Configuration Protocol (DHCP) allows the iConnectAccess624 to obtain an IP address automatically from the server. With dynamic addressing, a device may have a different IP address every time it connects to the network. This is not commonly used in Australia. Before configuration, please check with your DSL Provider / ISP to ensure that this mode is supported.

To Configure The iConnectAccess624 For A DHCP Connection:

From any screen in the web interface,

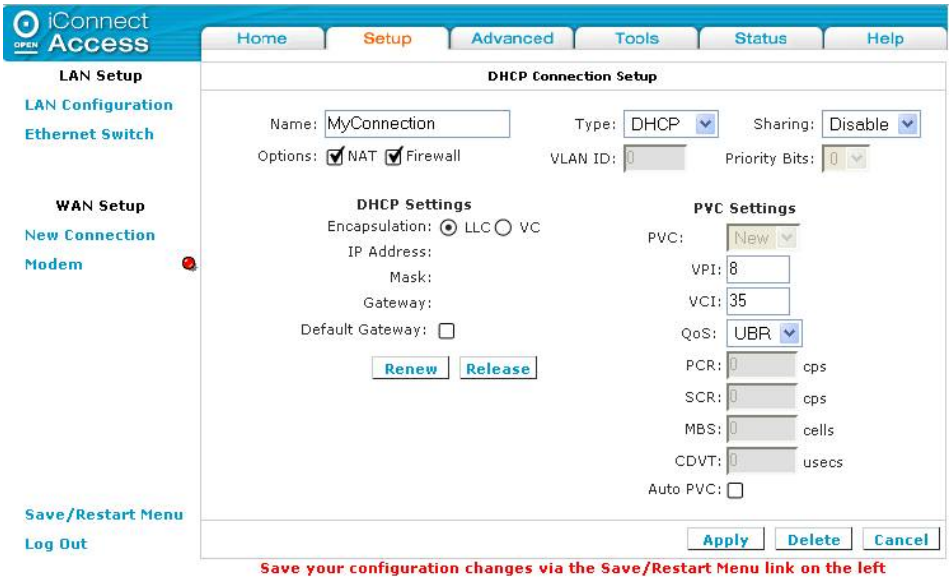
step 1 Click **Setup**.

step 2 From the *WAN Setup* menu, click **New Connection**.
The default *PPPoE Connection Setup* screen is displayed.

NOTE:

If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values.

step 3 From the *Type* drop-down list select *DHCP*. The following appears:



step 4 Enter a unique name for the DHCP Connection in the *Name* field. The name must not have spaces and cannot begin with numbers.

step 5 In the *Options* area of the screen, leave the *NAT* and *Firewall* checkboxes as default. (ie, checked.)

step 6 Select the encapsulation type (*LLC* or *VC*) by highlighting the appropriate radio button. If you are unsure leave the setting as default.

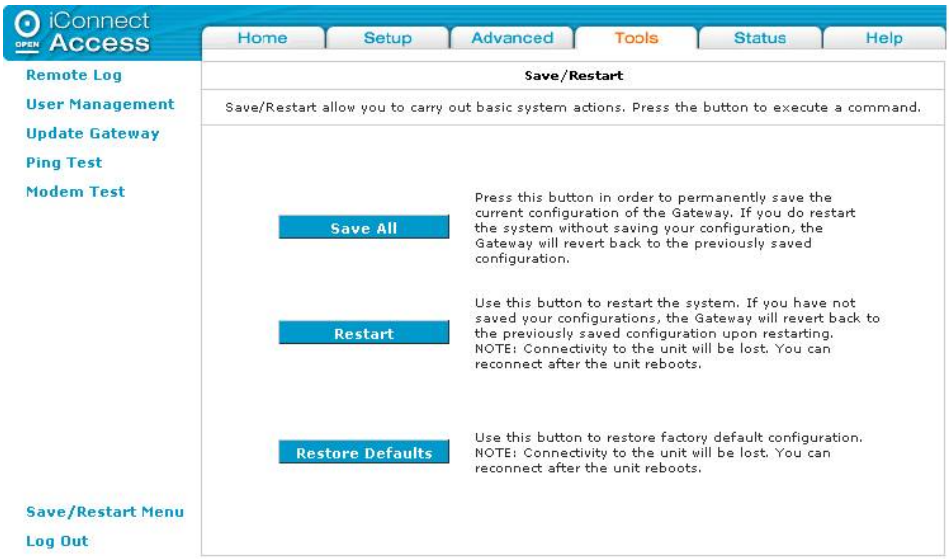
step 7 Enter the *VPI* and *VCI* settings as provided by your DSL Provider / ISP.

step 8 If your DSL line is connected and your DSL/ISP provider supports DHCP, click the **Renew** button to retrieve an IP address, Subnet mask, and Gateway address.

NOTE:

You can renew the DHCP address at any time by clicking **Renew**. *However, in most cases you will never need to use this button as the process runs automatically.*

step 9 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 10 Click **Save All** to save the changes permanently.

The following table lists the *DHCP Connection Setup* screen fields and their definitions:

Field	Description	
NAT	*Network Address Translation* is a feature that enables you to use private IP addresses on your computer or your LAN. This is set to *Enabled* by default for standard operation.	
Firewall	Check this checkbox to monitor traffic passing between your LAN and the outside world on this connection, to prevent security breaches. This is set to *Enabled* by default for standard operation.	
Encapsulation	LLC and VC are two different methods of encapsulating multiple sessions. This is set to *LLC* by default.	
	LLC	With LLC encapsulation, a link control header is added to the Ethernet packet that identifies the protocol type (Ethernet). This allows multiple protocols to be transmitted over the ATM Virtual Circuit.
	VC	With VC Multiplexing, no link control header is needed as the ATM Virtual Circuit is assumed to be carrying a single protocol.
Default Gateway	Check this checkbox to set this connection as the default gateway in the routing table.	
Renew	Sometimes it becomes necessary to get a new IP address or update DHCP options sent by a DHCP server. Pressing this button will renew the DHCP lease.	
Release	Clicking this button will release the current network settings from the iConnectAccess624.	
PVC	Select a PVC from the drop-down list.	
VPI	The *VPI (Virtual Path Identifier)* defines the virtual path settings for the ADSL connection between you and your ISP. The VPI value entered here must be supported by your ISP.	
VCI	The *VCI (Virtual Channel Identifier)* defines the virtual channel settings for	

Field	Description
	the ADSL connection between you and your ISP. The VCI value entered here must be supported by your ISP.
QoS	QoS defines iConnectAccess624 capabilities that provide guarantee of performance such as traffic delivery priority, speed, latency, or latency variation. Delivery of good-quality audio or video streams typically requires QoS capabilities. Three different quality of service options are available in the iConnectAccess624. These are UBR, CBR and VBR. The QoS selected here must be supported by your ISP. By default this is set to *UBR*.

Classical IP Over ATM (CLIP) Connection Set Up

Classical IP over ATM (CLIP), (defined in RFC1577) provides the ability to transmit IP packets over an ATM network, CLIP support will encapsulate IP in an AAL5 packet data unit (PDU) frame using RFC1577and it utilizes an ATM aware version of the ARP protocol.

To Configure The iConnectAccess624 For A CLIP Connection:

From any screen in the web interface,

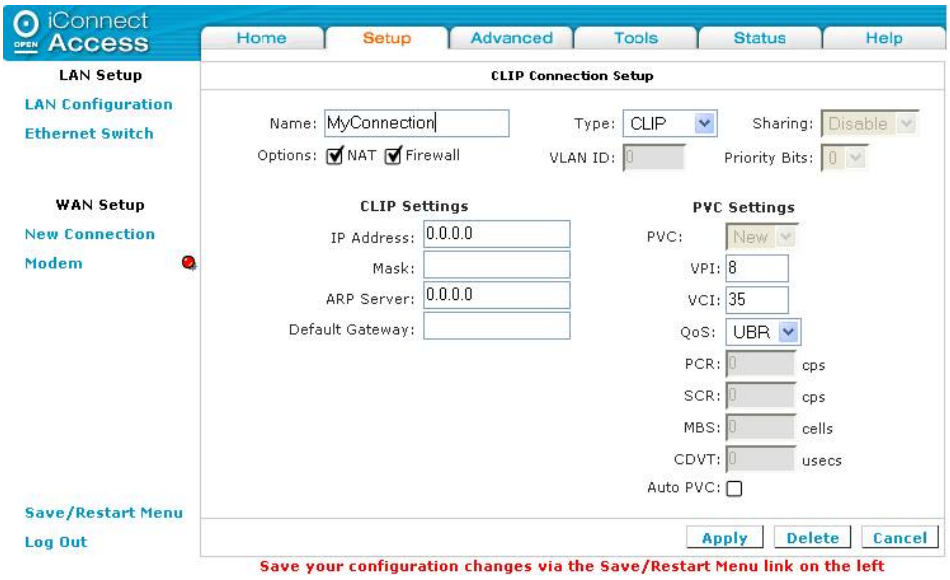
step 1 Click **Setup**.

step 2 From the *WAN Setup* menu, click **New Connection**.
The default *PPPoE Connection Setup* screen appears.

step 3 From the *Type* drop-down list select *CLIP*. The following appears:

NOTE:

If you need to use the VPI and VCI values in an existing connection, you will need to open it and edit the setting. It is not possible to have more than one connection using the same VPI/VCI values.



step 4 Enter a unique name for the CLIP connection in the *Name* field. The name must not have spaces and cannot begin with numbers.

step 5 Leave the *NAT* and *Firewall* options as the default settings. (ie, checked.)

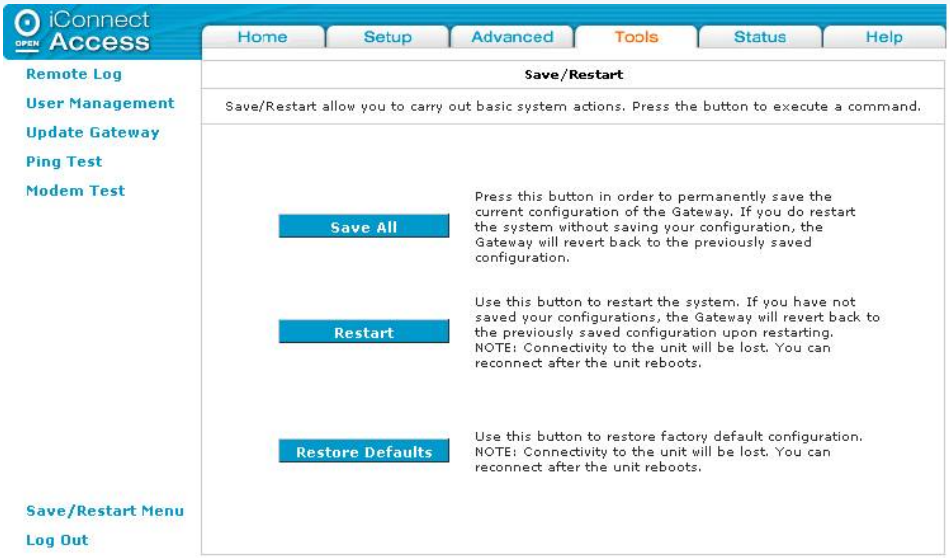
step 6 Enter the *VPI* and *VCI* settings as provided by your DSL Provider / ISP.

step 7 From the *Quality of Service (QoS)* drop-down list, select the QoS required, or if you are uncertain, leave the default value.

step 8 Enter the *CLIP Settings*, including *IP Address, Mask* and *Default Gateway* as provided by your DSL Provider / ISP.

step 9 Leave the *ARP Server* address as the default, unless advised by your DSL Provider / ISP.

step 10 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

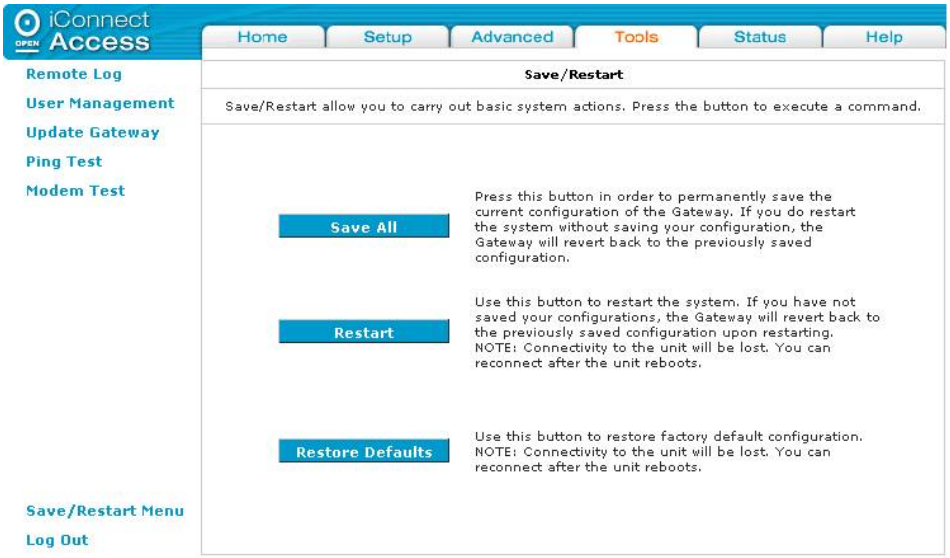
step 11 Click **Save All** to save the changes permanently.

Modify An Existing Connection

To Modify An Existing Connection:

From any web interface screen,

- Click **Setup**, then click the connection you wish to modify from the menu list. The connections are listed as their unique names.
- Edit as applicable and click **Apply**, or if you are deleting the entry, click **Delete,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

- Click **Save All** to save the changes permanently.

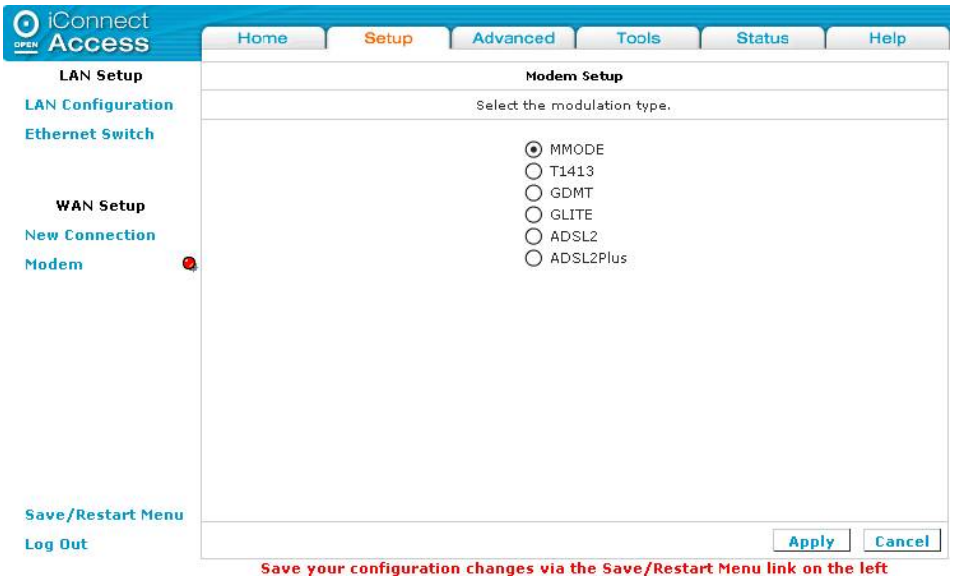
Modem Set Up

To Configure The DSL Modem Type:

From any web interface screen,

step 1 Click **Setup**.

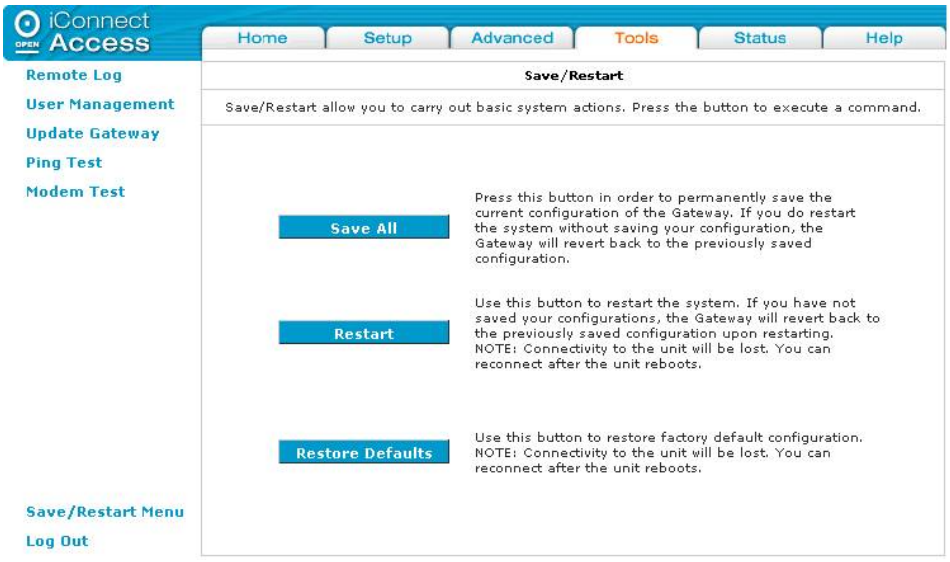
step 2 Under the *WAN Setup* menu, select **Modem**. The screen below appears. Leave the default setting if you are unsure of this value.



NOTE:

The iConnectAccess624 is pre-configured to detect the ADSL modulation standard automatically. In most cases, this screen should not be modified.

step 3 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart Menu
Log Out
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

step 4 Click **Save All** to save the changes permanently.

The following table lists the *ADSL Handshake* screen fields and their definitions:

Field	Description
T1413	ANSI T1.413-1998
GDMT	G.dmt (G.992.1)
GLITE	G.lite (G.992.2)
MMODE	Multi-Mode (the modulation is automatically detected)
ADSL	Asymmetric Digital Subscriber Line has the ability to transmit data at high speeds over a phone line while remaining available for (voice) phone use.
ADSL2Plus	ADSL delivering speeds up to 24Mbps.

Advanced Tab

The iConnectAccess624 supports a host of advanced networking and routing features including security, port configuration, and plug and play capability.

UPnP

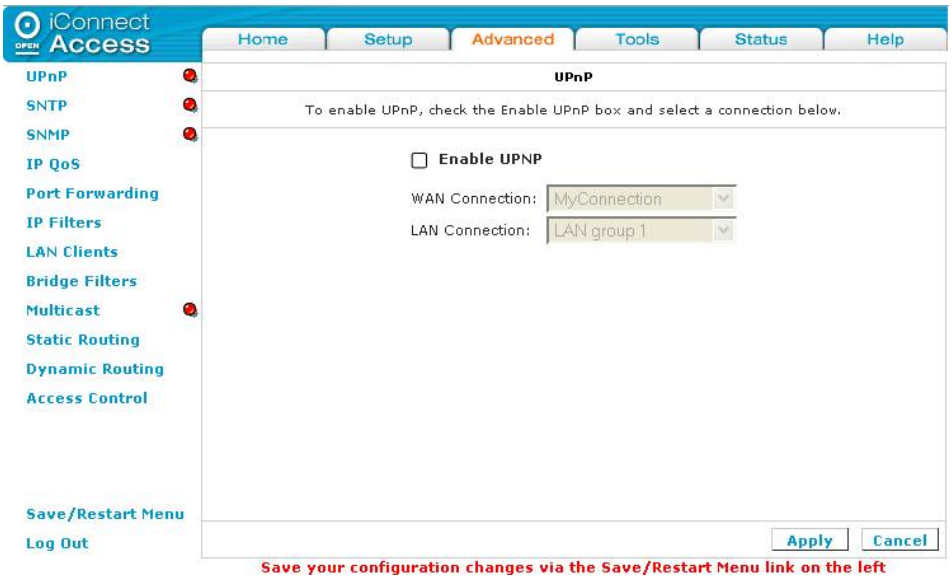
Universal Plug and Play is a networking architecture that provides compatibility among networking equipment, software and peripherals such as games consoles, digital cameras, and other systems that connect by TCP/IP. It can be supported on any operating system, and boasts device-driver independence and zero-configuration networking.

To Enable UPnP:

NOTE:
Before enabling UPnP, ensure that you have a WAN connection configured.

From any web interface screen,

step 1 Click **Advanced,** then **UPnP**. The following appears:

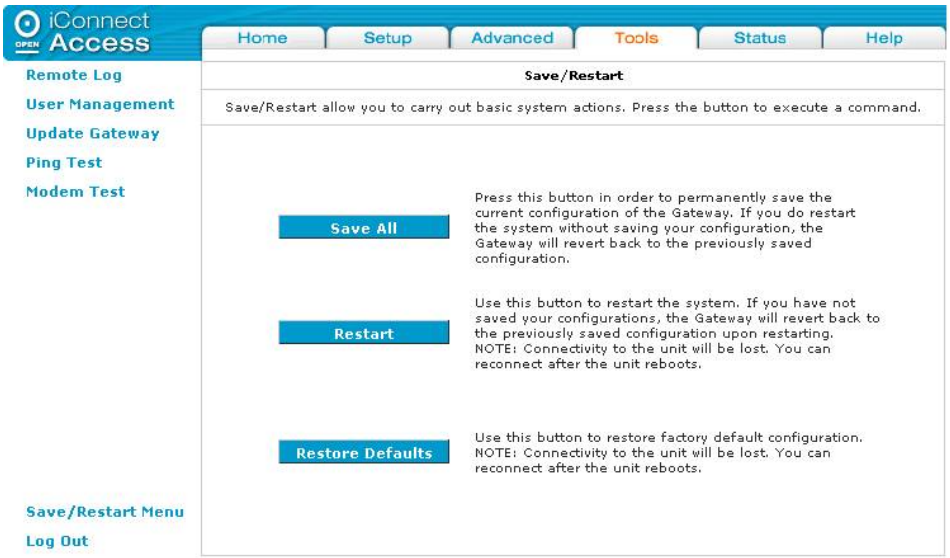


step 2 Check the *Enable UPnP* checkbox.

step 3 Select the required *WAN Connection* by highlighting the appropriate item from the drop-down list.

step 4 From the *LAN Connection* drop-down list, select the LAN connection as appropriate.

step 5 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 6 Click **Save All** to save the changes permanently.

The following table lists the *UPnP* screen fields and their definitions:

Field	Description
Enable UPNP	Universal Plug and Play (UPnP) is a standard that uses Internet and Web protocols to enable the iConnectAccess624 to be plugged into a network and automatically know about each other. With UPnP enabled, when a user plugs the iConnectAccess624 into the network, the device will configure itself, acquire a TCP/IP address, and use a discovery protocol based on the Internet's Hypertext Transfer Protocol (HTTP) to announce its presence on the network to other devices. This is set to *Disabled* by default in the iConnectAccess624.
WAN Connection	Select the WAN connection from the drop-down list of configured WAN connections.
LAN Connection	Select the LAN connection from the drop-down list of available LAN Group connections.

NOTE:
UPnP can only be enabled on a saved Configuration File.

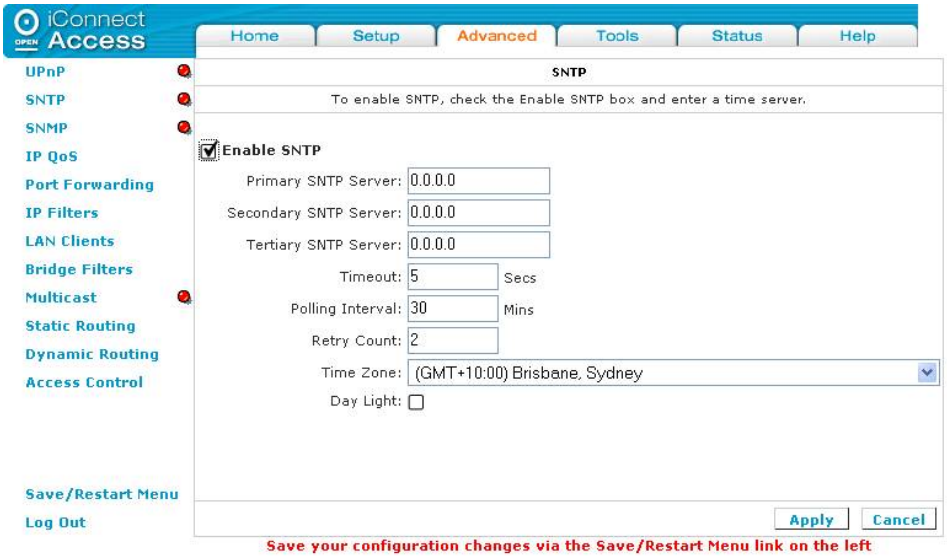
SNTP

Simple Time Network Protocol ensures that computer clock times can be synchronised in a network of computers to the millisecond.

To Configure SNTP For The iConnectAccess624:

From any web interface screen,

step 1 Click **Advanced**, then **SNTP**. The following appears:



step 2 Click the *Enable SNTP* checkbox.

step 3 Enter a primary SNTP Server address as required in the *Primary SNTP Server* field.

step 4 Repeat step 3 for the Secondary and Tertiary SNTP Server addresses as required.

step 5 Enter a timeout limit (in seconds) in the *Timeout* field.

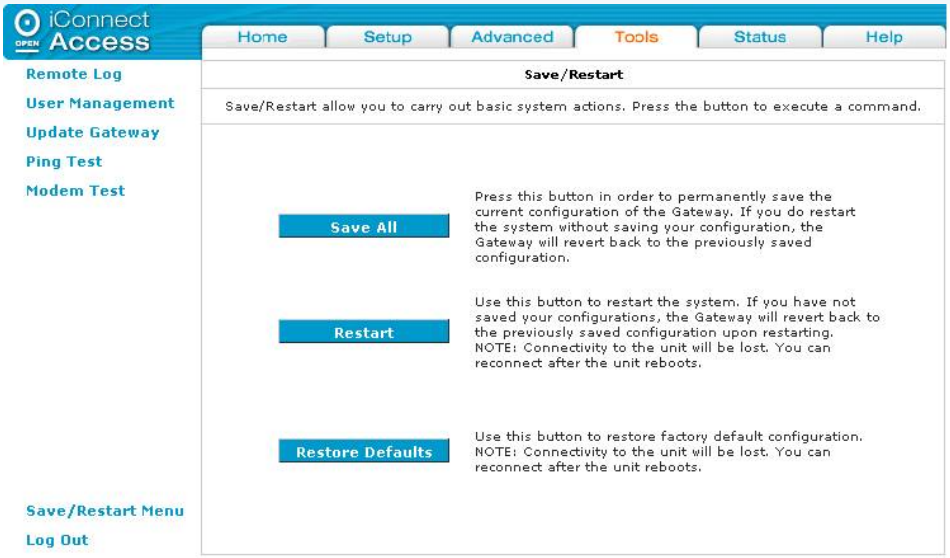
step 6 Enter a Polling Interval limit (in minutes) in the *Polling Interval* field.

step 7 Enter the number of times to retry connecting to the server in the *Retry Count* field.

step 8 From the *Time Zone* drop-down list, select the time zone in which the router is operating.

step 9 Check the *Day Light* checkbox to activate daylight savings time.

step 10 Click **Apply**, then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 11 Click **Save All** to save the changes permanently.

The following table lists the *SNTP screen* fields and their definitions:

Field	Description
Enable SNTP	Check this checkbox to enable the iConnectAccess624 to synchronise its system time to an external time source.
Primary SNTP Server	The IP Address or fully qualified name of the time source.
Secondary SNTP Server	The IP Address or fully qualified name of a backup time source.
Tertiary SNTP Server	The IP Address or fully qualified name of a backup time source.
Timeout	Time in seconds that the iConnectAccess624 will wait for an SNTP server to respond.
Polling Interval	Polling period in minutes that the iConnectAccess624 checks time with the SNTP server.
Retry Count	Number of retries before a backup server is polled.
Time Zone	Select the time zone in which your network is operating from this drop-down list.
Day Light	Check the *Day Light* check box to activate daylight savings time.

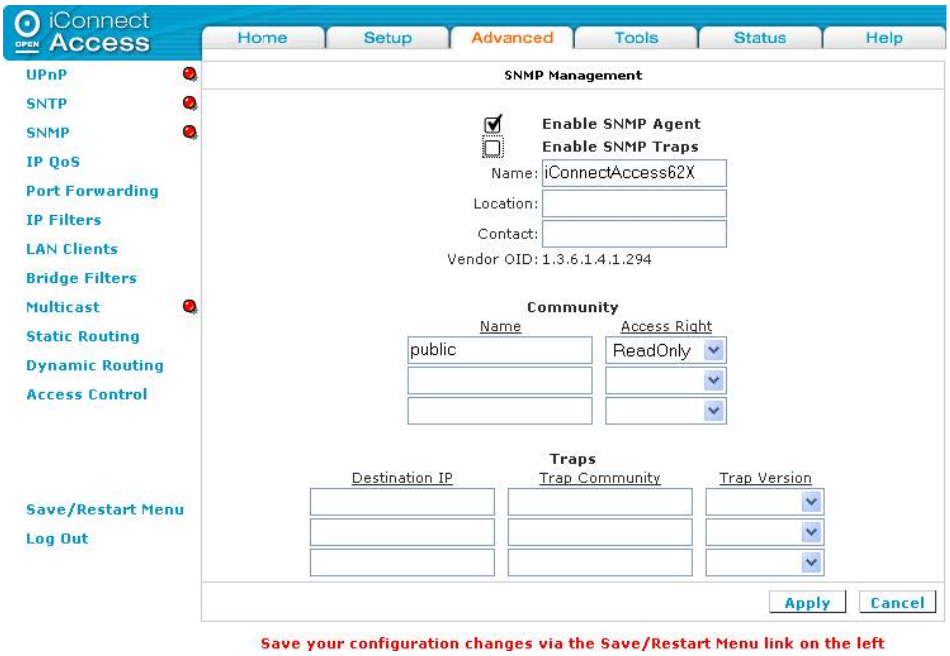
SNMP

SNMP stands for Simple Network Management Protocol. It is used to monitor the state of the network remotely, collecting information about Internet traffic events and device status and storing these in a database. For example, SNMP can be used to monitor the amount of traffic passing through the network.

To Configure SNMP Details:

From any web interface screen,

step 1 Click **Advanced,** then **SNMP**. The following appears:



step 2 Check the *Enable SNMP Agent* and *SNMP Traps* checkboxes.

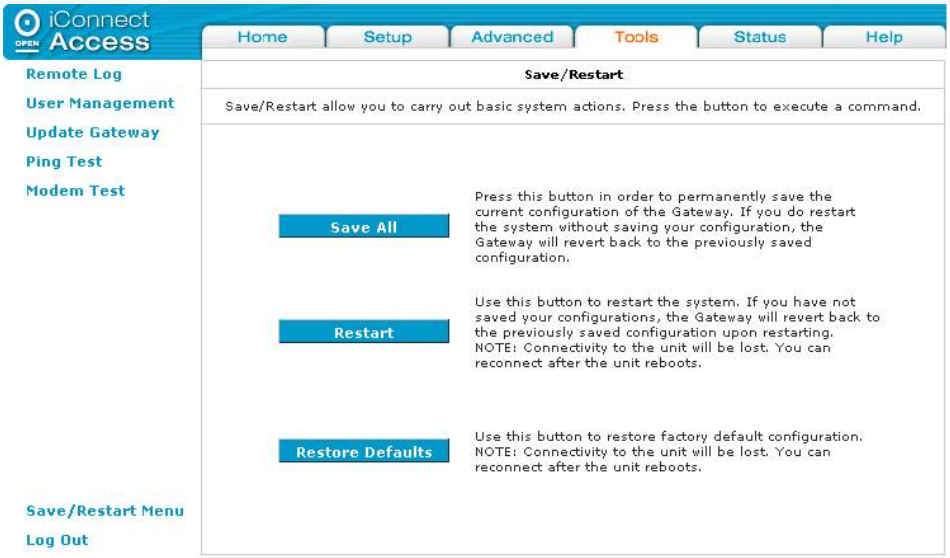
step 3 Enter a name for the device in the *Name* field.

step 4 Enter the vendor's location in the *Location* field.

step 5 Enter a contact for the vendor in the *Contact* field.

step 6 Enter a community name in the *Name* field in the *Community* area of the screen, for *Read-Only* access. The default is *Public*.

step 7 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 8 Click **Save All** to save the changes permanently.

The following table lists the *SNMP Management* screen fields and their definitions:

Field	Description
Enable SNMP Agent	Check this checkbox to enable SNMP (Simple Network Management Protocol) on this device. Enter the SNMP settings in the *Community* area of the screen.
Enable SNMP Traps	Check this checkbox to enable the SNMP trap service. Enter the SNMP trap settings in the *Traps* area of the screen.
Traps Destination IP	Enter the Destination Address of the host to receive the SNMP traps.
Trap Community	Enter the Community name in this field. This should match the community name on the server receiving the traps.
Trap Version	Select the version of SNMP to use from this drop-down list.
SNMP Management (Name, Location, Contact)	Enter details specific for this device in the *Name, Location* and *Contact* fields.
Community Name and Access Rights	The SNMP Read-Only Community string is like a User-ID or Password that allows access to the router's statistics. SNMP Read-Write Community String allows a remote device to read information from a device, and to modify settings on that device. If using SNMP Read-Write do not leave this password at the default.

IP QoS

Before attempting to configure IP QoS, you will need a good understanding of the TCP/IP protocol and ports.

The IP Quality Of Service (QoS) queues data streams to ensure that basic connectivity is maintained when running multiple services over one connection. For example, if you are using a peer-to-peer file-sharing program whilst simultaneously performing normal web browsing, you can configure QoS to limit the resources dedicated to the peer-to-peer session to ensure web browser connectivity. IP QoS is often critical to maintain VoIP session quality.

IP QoS services in the iConnectAccess624 are applicable to the output device (LAN side). This means that the IP QoS is associated with any transmitted traffic from the iConnectAccess624. Each output device has three priority queues associated with transmit data. The High priority queue has strict priority over medium and low priority queues. The Medium and Low priority queues are serviced on a round robin priority basis according to the configured weights (WRR), after the High priority queue has been completely serviced.

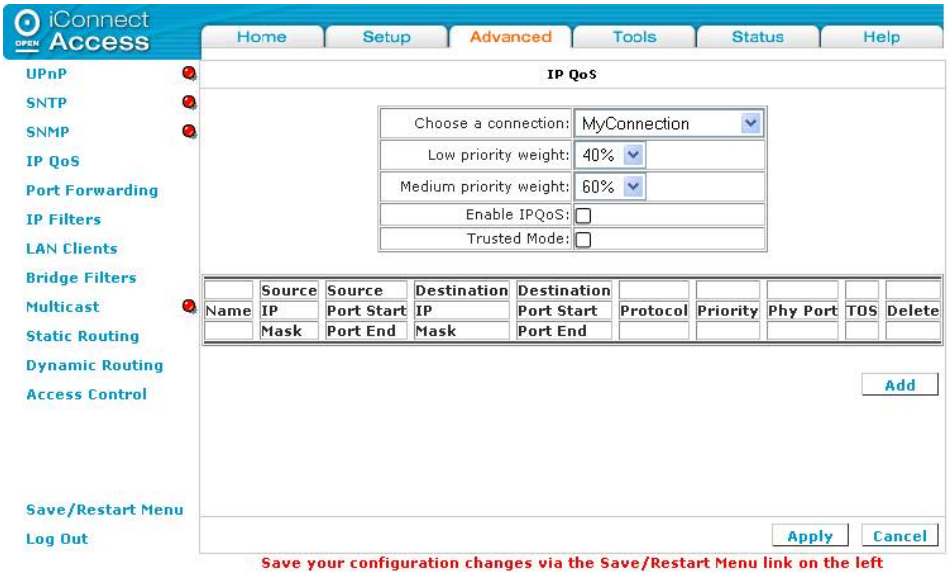
NOTE:

If IP QoS is enabled and no rules are defined, a default rule is added which is hidden. The default rule places all traffic to be transmitted in the Low priority queue.

To Configure IP QoS:

From any web interface screen,

step 1 Click **Advanced,** then **IP QoS.** The following screen appears:



step 2 Select a WAN connection to enable IP QoS for the modem's upstream traffic, or choose a LAN connection (Ethernet) for the downstream traffic, from the *Choose a connection* drop-down list.

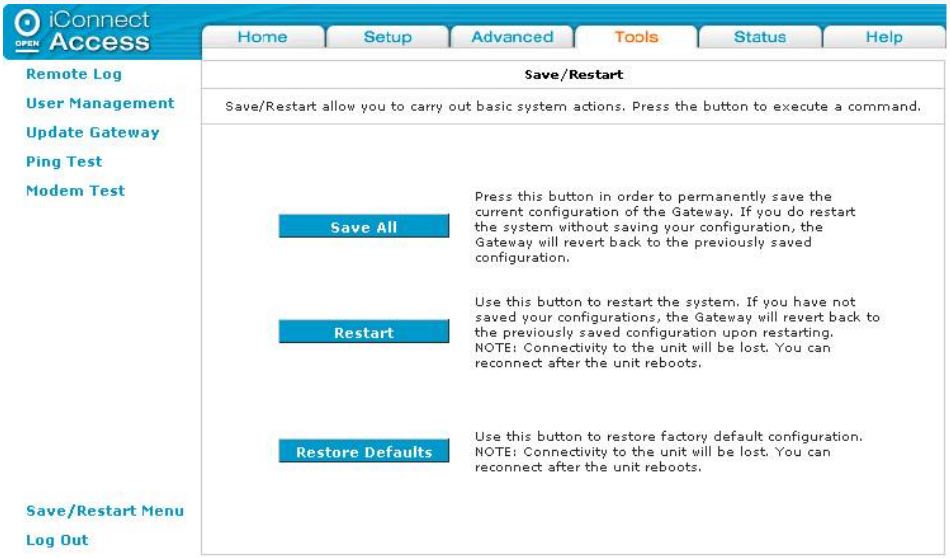
step 3 Select a percentage from the *Low priority weight* drop-down list.

step 4 Select a percentage from the *Medium priority weight* drop-down list.

step 5 If you wish to enable IP QoS, check the *Enable IPQoS* checkbox.

step 6 If you wish to enable trusted mode, check the *Trusted Mode* checkbox.

step 7 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 8 Click **Save All** to save the changes permanently.

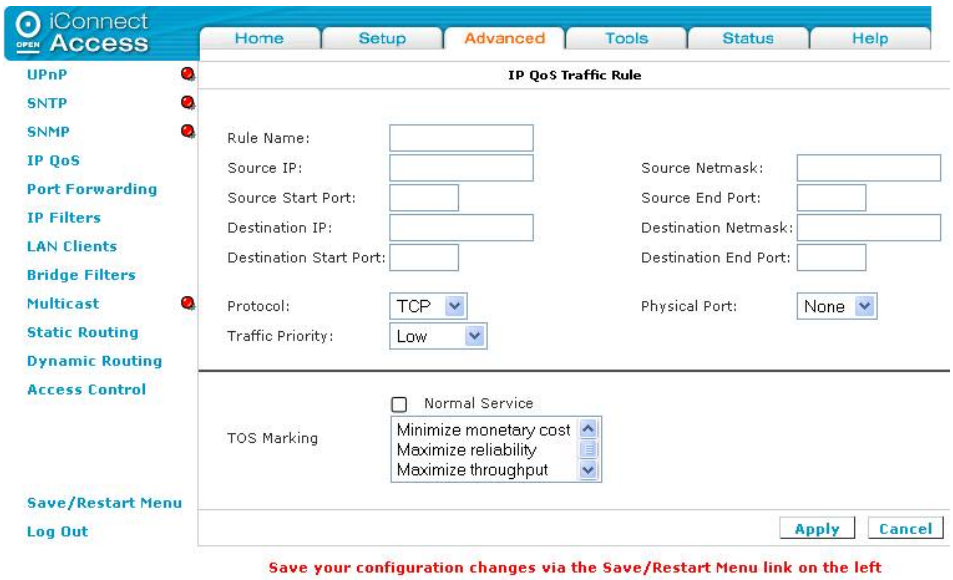
The following table lists the *IP QoS* screen fields and their definitions:

Field	Description
Choose a Connection	This lists the connection names that are configured on the iConnectAccess624. Select a WAN or LAN connection here.
Low Priority Weight / Medium Priority Weight	These two fields allow you to select the weights of the Medium and Low Priority queues in increments of 10 percent, so that the sum of the weights is 100 percent.
Enable IP QoS	Check /uncheck this checkbox to enable / disable IP QoS for the selected connection.
Trusted Mode	The iConnectAccess624 has two primary modes of operation: Trusted and Untrusted. *Trusted*: In Trusted mode, all the rules will be applied first, regardless of the Type Of Service (TOS) bit setting. (After the rules have been exhausted, the existing TOS bit settings will be honoured.) *Untrusted*: Untrusted Mode matches first against all rules, as in Trusted Mode. If there is no match, then a default rule will be used. The queuing priority of the default rule is Low.

To Define IP QoS Traffic Rules:

The IP QoS page appears when you click the **Add** button in the *QoS Setup* screen. When setting rules, each rule is a matching criterion that identifies the application traffic to be transmitted by the iConnectAccess624 using one of the three priority queues – High, Medium or Low.

step 1 From the *IP QoS* screen, click **Add** to define the IP QoS traffic rules. The following screen appears:



step 2 Enter a rule name in the *Rule Name* field.

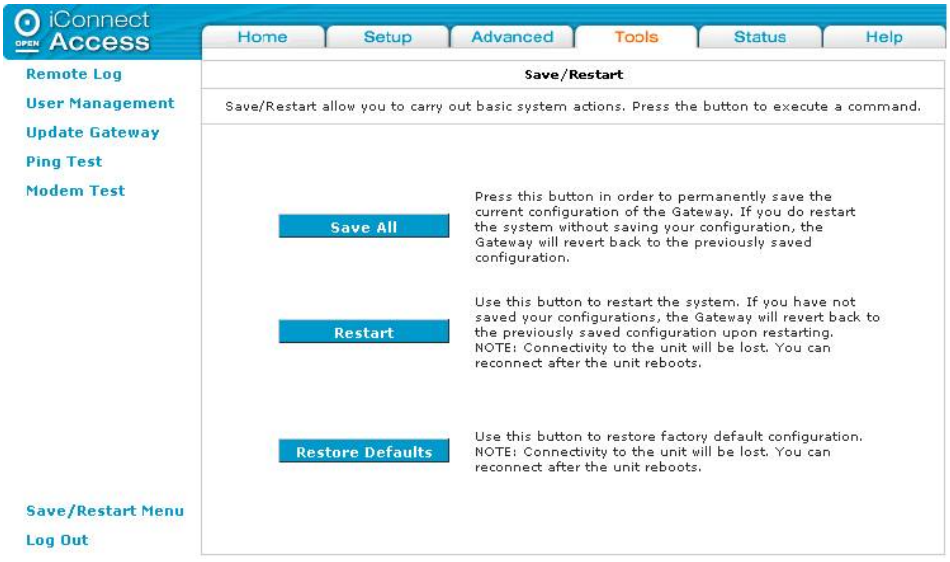
step 3 Identify the traffic by source and destination IP address and ports.

step 4 Select the protocol from the *Protocol* drop-down list. The options are: *TCP, UDP, ICMP* or *ANY*.

step 5 Select the priority queue in which the identified traffic will be placed, from the *Traffic Priority* drop-down list. The options are: *Low*, *Medium*, or *High*.

step 6 If you wish to set the TOS bit, select it from the *TOS Marking* drop-down list.

step 7 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart Menu
Log Out
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

step 8 Click **Save All** to save the changes permanently.

The following table lists the *IP QoS Traffic Rule* screen fields and their definitions:

Field	Description
Rule Name	This lists the connection names that are configured in the iConnectAccess624.
Source IP	The IP address of the device that is the sending the information.
Source Netmask	The Network Mask of the device that is sending the information.
Source Start Port /Source End Port	The port number/port range of device that is sending the information on. The port range must be between 1 – 65535.
Destination IP	The IP address of the device that is the receiving the information.
Destination Netmask	The Network Mask of the device that is receiving the information.
Destination Start Port Destination End Port	The port number/port range of device that is receiving the information on. The port range must be between 1 – 65535.
Protocol	Select the protocol for your traffic. The options are: *TCP, UDP, ICMP* or *ANY*.
Traffic Priority	This is the priority for the source traffic. The options are: *Low*, *Medium* or *High* for the selected traffic.
Normal Service TOS Marking	The additional TOS marking field allows you to assign a Type Of Service (TOS) value to this traffic. The values for the TOS marking are: *No Change, Normal Service, Minimise Monetary Cost, Maximise Reliability, Maximise Throughput* and *Minimise Delay*.

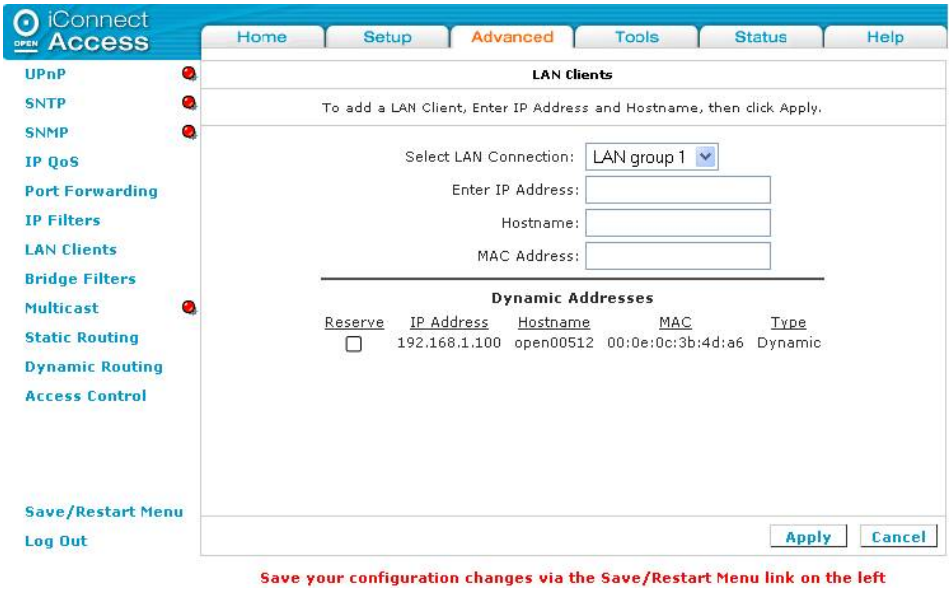
LAN Clients

If DHCP is used, all current DHCP clients are automatically registered in the LAN Client database. However, if a Static IP Address is used on a LAN device and you need this to be visible via the WAN, you must add its IP address to the LAN Clients list. Once the IP address has been added you will be able to apply Port Forwarding, IP Filtering and QoS rules to it.

To Add A LAN Client:

From any web interface screen,

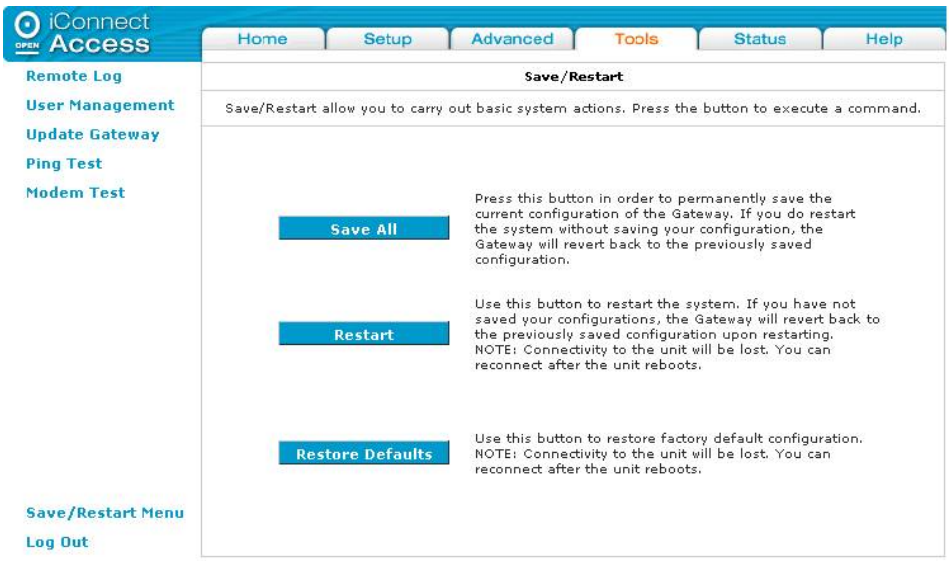
step 1 Click **Advanced**, then **LAN Clients**. The following screen appears:



step 2 Enter the LAN IP Address in the *Enter IP Address* field.

step 3 Enter the LAN's hostname in the *Hostname* field if required.

step 4 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart Menu
Log Out
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.

step 5 Click **Save All** to save the changes permanently.

NOTE:

Once the IP Address has been added you are now able to apply Port Forwarding and Access Control rules to it.

The following table lists the *LAN Clients* screen fields and their definitions:

Field	Description
Select LAN Connection:	The LAN group to which you are adding the new LAN client.
Enter IP Address	IP address of the server/host that you want to use for port forwarding or access control must be defined here.
Hostname	An optional hostname can be assigned to the above address.

Bridge Filters

The Bridge filtering mechanism enables users to define rules which allow/deny access through the iConnectAccess624 via the hardware (MAC Address) of network devices.

The User Interface for Bridge Filter allows the following functionality:

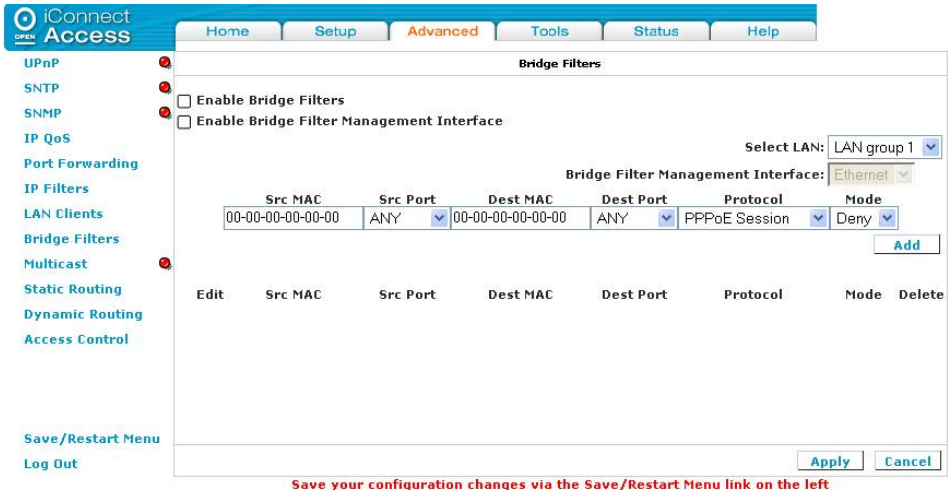
- Adding/Editing/Deleting filter rules;
- Enabling filter rules.

To Enable Bridge Filters:

The *Enable Bridge Filters* checkbox allows the user to enable or disable Bridge filtering. It can be checked / unchecked during any editing operation. It can also be set/unset independently by just pressing the **Apply** button.

From any web interface screen,

step 1 Click **Advanced,** then **Bridge Filters**. The following screen appears:



step 2 Check the *Enable Bridge Filters* checkbox.

step 3 Check the *Enable Bridge Filter Management Interface* checkbox, then click **Apply**. You can now select the bridge filter management interface from the *Bridge Filter Management Interface* drop-down list.

step 4 If more than one LAN group has been created, select the LAN group filter to which the filter rules are to be applied.

step 5 Enter the source MAC address in the *Src MAC* field.

step 6 Select the source Port from the *Src Port* drop-down list.

step 7 Enter the destination MAC address in the *Destination MAC* field.

step 8 Select the destination Port from the *Dest Port* drop-down list.

NOTE:

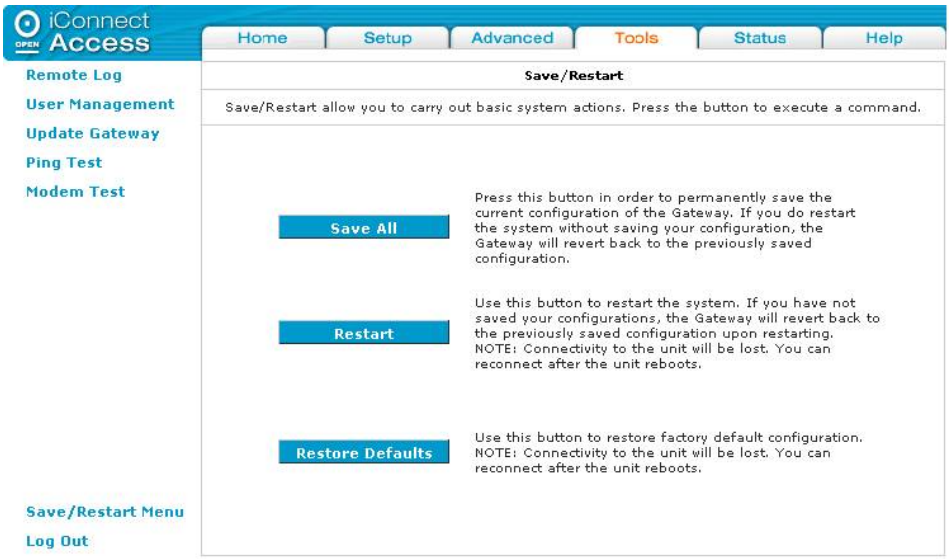
Entering 0s or blanks in the Source *or* Destination *fields means ALL MAC Addresses are specified.*

step 9 Select the protocol to be used from the *Protocol* drop-down list.

step 10 Select the mode with desired filtering type from the *Mode* drop-down list. The options are *Allow* or *Deny*.

step 11 Click **Add**.

step 12 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 13 Click **Save All** to save the changes permanently.

To Edit An Existing Filter Rule:

- From the *Bridge Filters* screen, highlight the *Edit* radio button for the rule to be edited, from the list of existing filter rules.
  The rule appears in the *Enable Bridge Filters* area of the screen.
- Make the required change / s to the *MAC Address, Protocol* and *Mode* types, and click **Apply.**

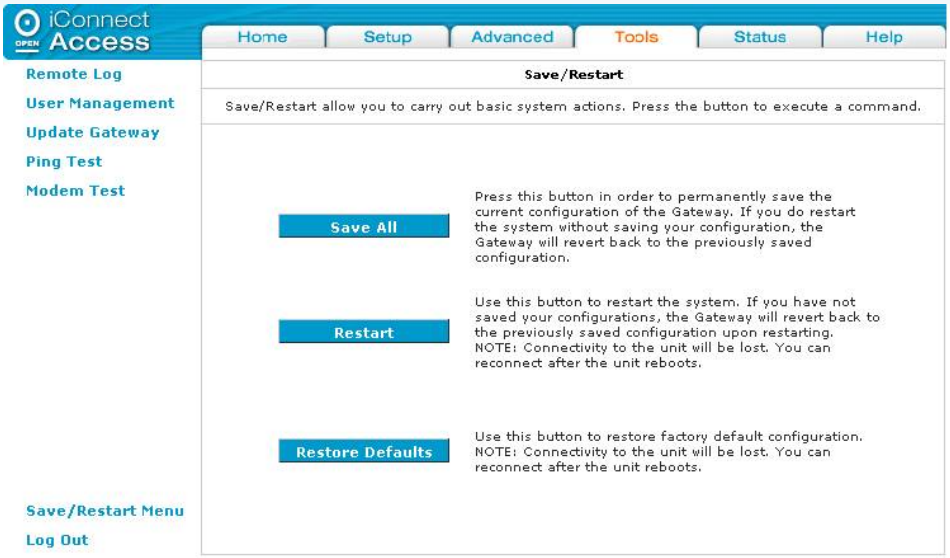
To Delete Filter Rule(s):

- Check the *Delete* checkbox beside the filter rule / s to be deleted.

NOTE:

Multiple deletions are possible by using the **<Shift>** *key and clicking the* Delete *checkboxes. The* Select All *checkbox can be used to delete all filter rules quickly.*

- Click **Apply**, then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

- Click **Save All** to save the changes permanently.

Hidden Bridge Filter Rules:

The Bridge filter table contains 3 hidden rules, which are entered automatically by the system to ensure you do not "lock" yourself out of the system. These include:

- Any ARP frames are permitted to pass through the system.
- All IPv4 frames with the destination MAC address of the bridge are permitted to pass through.
- All IPv4 frames with the source MAC address of the bridge are permitted to pass through.

NOTE:

To locate the MAC Address of a Windows-based machine, type `ipconfig /all` *at a DOS prompt.*

Multicast

Multicasting is a form of limited broadcast. UDP is used to send datagrams to all hosts that belong to what is called a "host group." A host group is a set of one or more hosts identified by the same destination IP address. The following statements apply to host groups.

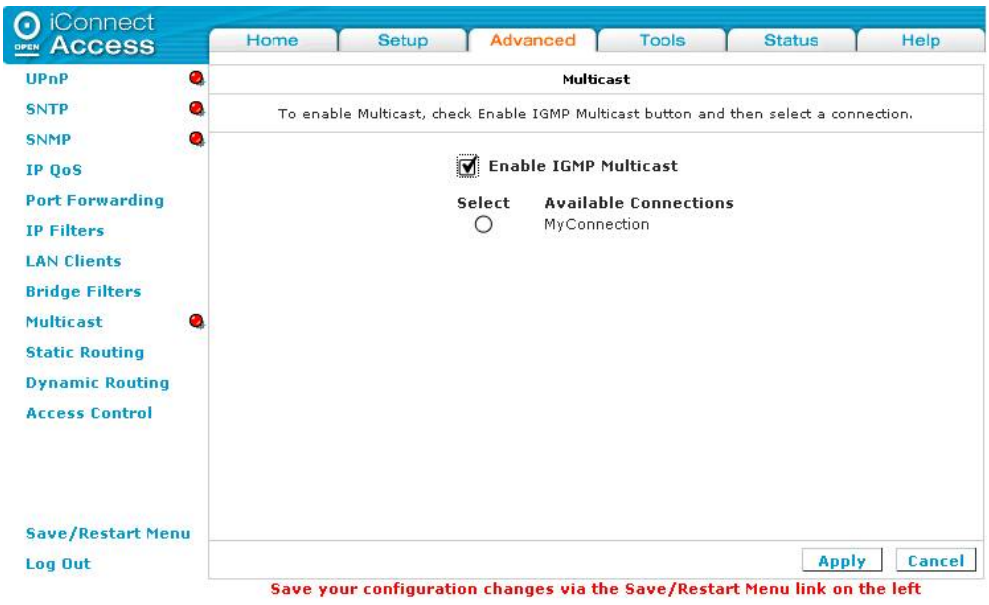
- Anyone can join or leave a host group at will;
- There are no restrictions on a host's location;
- There are no restrictions on the number of members that may belong to a host group;
- A host may belong to multiple host groups;
- Non-group members may send UDP datagrams to the host group.

Multicasting is useful when data needs to be sent to more than one other device. For instance, if one device is responsible for acquiring data that many other devices need, then multicasting is a natural fit. Note that using multicasting as opposed to sending the same data to individual devices uses less network bandwidth.

To Enable Multicasting:

From any web interface screen,

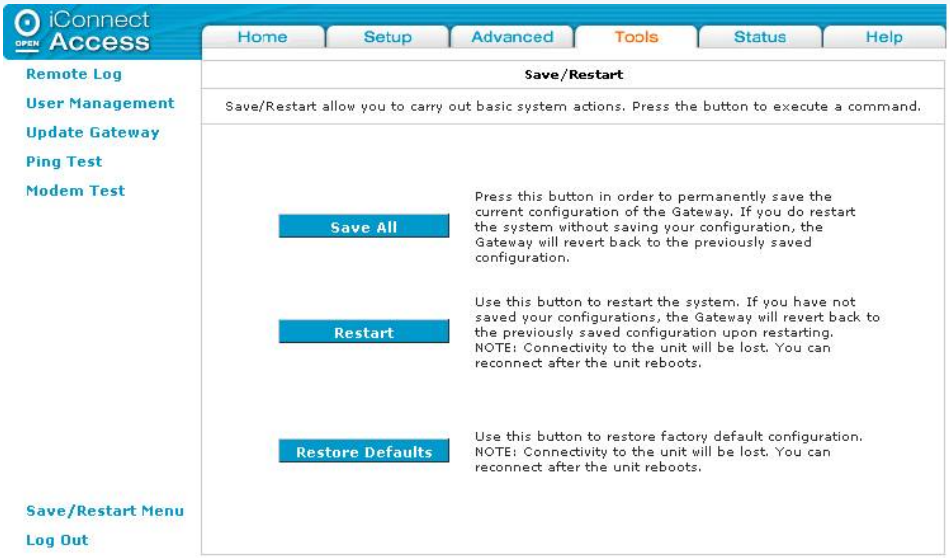
step 1 Click the **Advanced** tab, then **Multicast**. The following screen appears:



step 2 Check and / or highlight the *Enable IGMP Multicast* checkbox.

step 3 From the *Available Connections* area of the screen, highlight the *Select* radio button for the connection required.

step 4 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 5 Click **Save All** to save the changes permanently.

The following table lists the *Multicast* screen fields and their definitions:

Field	Description
Enable IGMP Multicast	IP packets are transmitted in one of two ways: ■ Unicast (1 sender to 1 recipient) or ■ Broadcast (1 sender to everybody on the network). Multicast delivers IP packets to just a group of hosts on the network. *IGMP (Internet Group Multicast Protocol)* is a session-layer (layer-3) protocol used to establish membership in a Multicast group. Checking this will enable the iConnectAccess624 to receive multicast traffic. Refer to RFC 1112 and RFC 2236 for information on IGMP versions 1 and 2 respectively.
Select Available Connections	Select the connection type here.

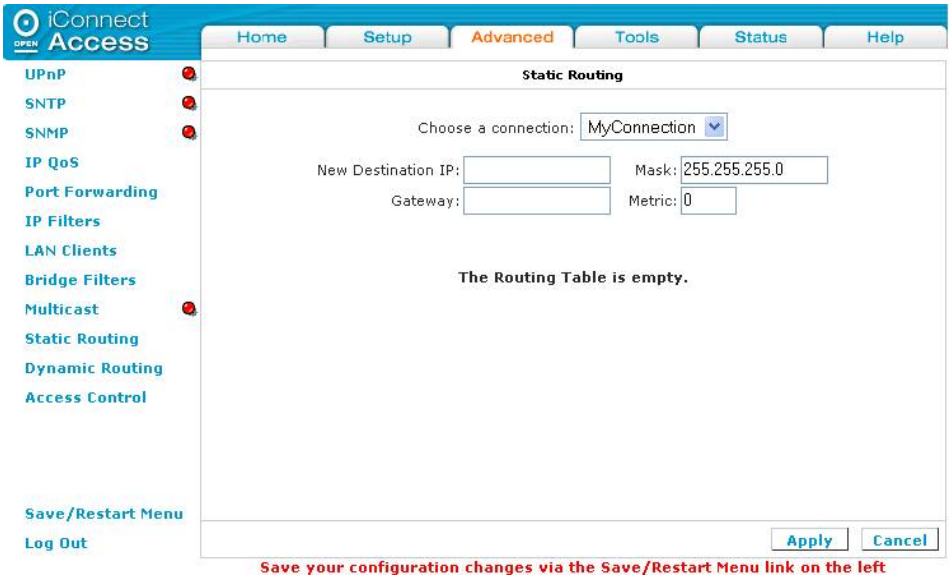
Static Routing

If the iConnectAccess624 is connected to more than one network, you may need to set up a static route between them. A static route is a pre-defined pathway down which network information must travel to reach a specific host or network. You can use static routing to allow different IP domain users to access the Internet through the iConnectAccess624.

To Enable Static Routing:

From any screen in the web interface,

step 1 Click **Advanced,** then **Static Routing**. The following screen appears:



step 2 From the *Choose a connection* drop-down list, select a connection type.

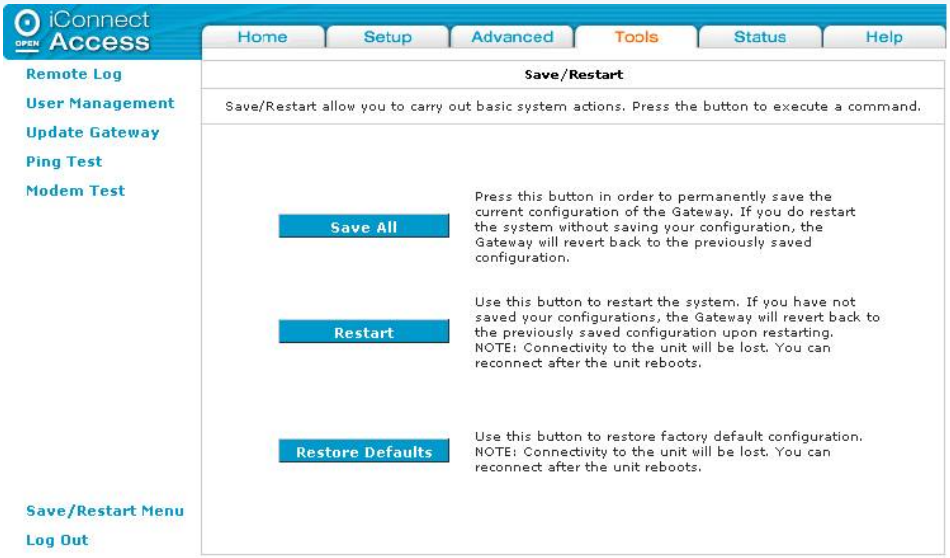
step 3 Enter the new destination IP for the remote LAN network or host to which you wish to assign a static route in the *New Destination IP* field.

step 4 Enter a subnet mask in the *Mask* field.

step 5 Enter the IP address of the near device to connection with the remote network or host in the *Gateway* field.

step 6 Enter a metric in the *Metric* field.

step 7 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 8 Click **Save All** to save the changes permanently.

The following table lists the *Static Routing* screen fields and their definitions:

Field	Description
Choose a Connection	Choose the connection profile from the drop-down list.
New Destination IP	This is the destination network or Host IP to which packets will be sent.
Mask	A mask used to determine the subnet to which an IP address belongs. This is the mask that determines the destination network.
Gateway	This is the IP address of the next hop router in the path of the destination network. When a packet is ready to be sent to a destination, the iConnectAccess624 sends it on to the Gateway. The gateway examines the destination address in the header and passes the packet along to another router, chosen by a route-finding algorithm. A packet may go through 30 or more routers in its travels from one host computer to another. Because routes are dynamically updated, it is possible for different packets from a single session to take different routes to the destination.
Metric	Metric (hop count) is used to measure the distance between the source and a destination network. Each hop in a path from source to destination is assigned a hop count value, which is typically 1.

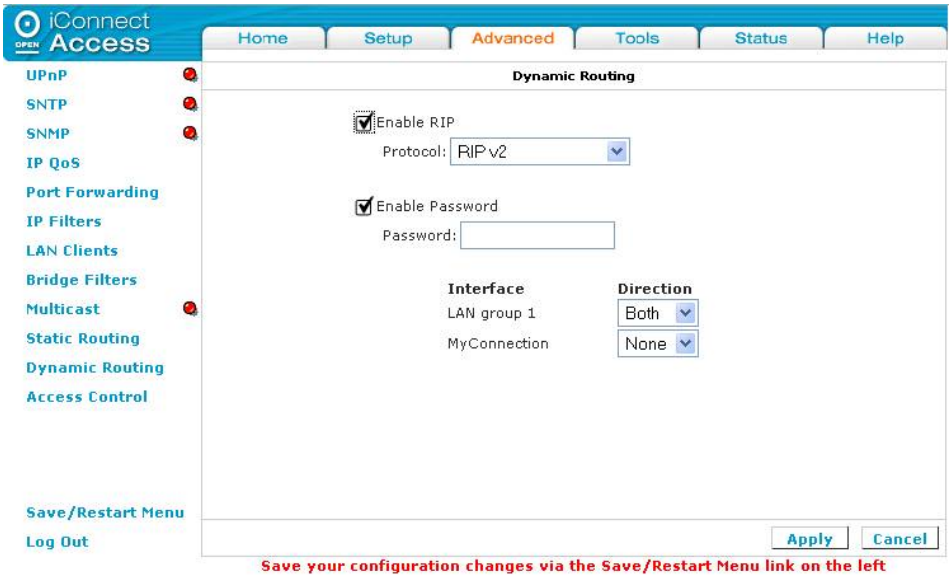
Dynamic Routing

Using Routing Information Protocol (RIP), dynamic routing allows the iConnectAccess624 to adjust to physical changes in the network automatically. It determines the route through which the packets travel based on the fewest number of hops between the source and destination. RIP protocol regularly broadcasts routing information to other Routers on the network.

To Enable Dynamic Routing:

From any web interface screen,

step 1 Click **Advanced,** then **Dynamic Routing**. The following screen appears:



step 2 Check the *Enable RIP* checkbox.

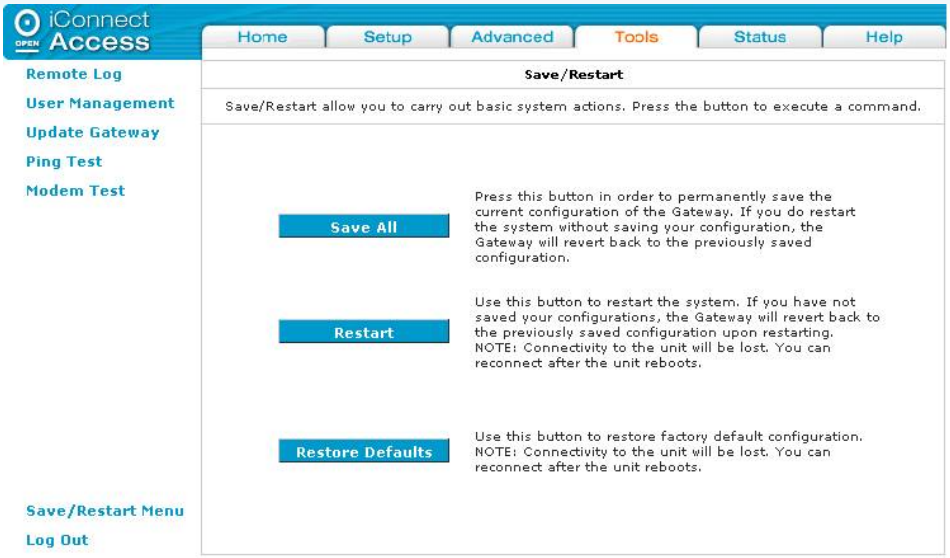
step 3 From the *Protocol* drop-down list, select the RIP version as appropriate.

step 4 Select the direction for the interface required from the *Direction* drop-down list.

step 5 Check / Uncheck the *Enable Password* checkbox as appropriate.

step 6 If you have checked the *Enable Password* checkbox, enter a password in the *Password* field.

step 7 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 8 Click **Save All** to save the changes permanently.

The following table lists the *Dynamic Routing* screen fields and their definitions:

Field	Description
Enable RIP	This enables RIP routing on the iConnectAccess624 router.
Protocol	There are two versions of RIP. RIP version 1 (v1) is defined in RFC 1058. RIP version 2 (v2) is defined in RFC 1723. Select between RIPv1, RIPv2 and RIPv1 compatible. The protocol is dependent upon the entire network. Most networks support RIP v1. If RIP v1 is selected, routing data will be sent in RIP v1 format. If RIP V2 is selected, routing data will be sent in RIP v2 format using subnet broadcasting. If RIP V1-Compatible is selected, routing data will be sent in RIP v2 format using multicasting.
Direction	The direction determines the means through which RIP routes will be updated. Selecting `In` means that the iConnectAccess624 will only incorporate received RIP information. Selecting `Out` means that the iConnectAccess624 will only send out RIP information. Selecting *Both* means that the iConnectAccess624 will incorporate received RIP information and send out updated RIP information.
Enable Password	Simple password authentication for RIPv2 was defined in RFC 1723. If you intend to use password authentication you must enable your password here.
Password	Type the RIPv2 authentication password here. Ensure that all routers are configured with this password for RIPv2 to work.

Firewall

In the presence of the firewall, anonymous Internet traffic is blocked. Using advanced security features, you can redirect this traffic to a dedicated computer on your local network Demilitarised Zone (DMZ) or open access from the Internet to the iConnectAccess624 management ports (web, Telnet). The iConnectAccess624's firewall and NAT services (port forwarding, access control) can be disabled for all interfaces by unchecking the *Enable Firewall* and *NAT Service* checkboxes.

Port Forwarding

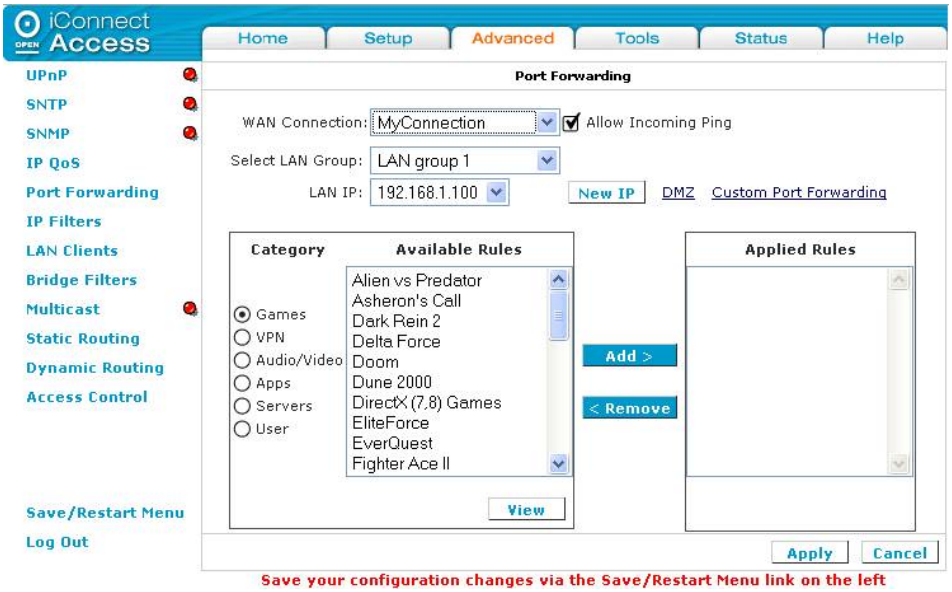
Using the Port Forwarding page, you can provide local services (for example web hosting) for people on the Internet, or play Internet games. When users send this type of request to your network via the Internet, the iConnectAccess624 will forward those requests to the appropriate computer. Port Forwarding can be used with DHCP-assigned addresses but remember that a DHCP address is dynamic (not static). For example, if you were configuring a Netmeeting server, you would want to assign this server a static IP address so that the IP address is not reassigned. Also remember that if an Internet user is trying to access an Internet application, they must use the WAN IP address. Port forwarding will translate the WAN IP address into a LAN IP address.

Configuring Port Forwarding is a two-part process. Firstly you must ensure that you have a LAN IP Address configured in LAN Clients, and once you have completed this, you can then configure Port Forwarding.

To Configure Port Forwarding:

From any screen in the web interface,

step 1 Click **Advanced**, then **Port Forwarding**. The following screen appears:



step 2 From the *WAN Connection* drop-down list, select the connection type for which you wish to add the firewall rule.

step 3 From the *Select LAN Group:* drop-down list, select the LAN group for which you wish to add the firewall rule.

step 4 From the *Select LAN Group:* drop-down list, select the LAN group for which you wish to apply the rule.

step 5 From the *LAN IP* drop-down list, select the IP address for which you wish to apply the rule. If you wish to add a new LAN IP address, highlight the user category and click **New IP** button, and follow the instructions in *To Add A LAN Client:*.

NOTE:

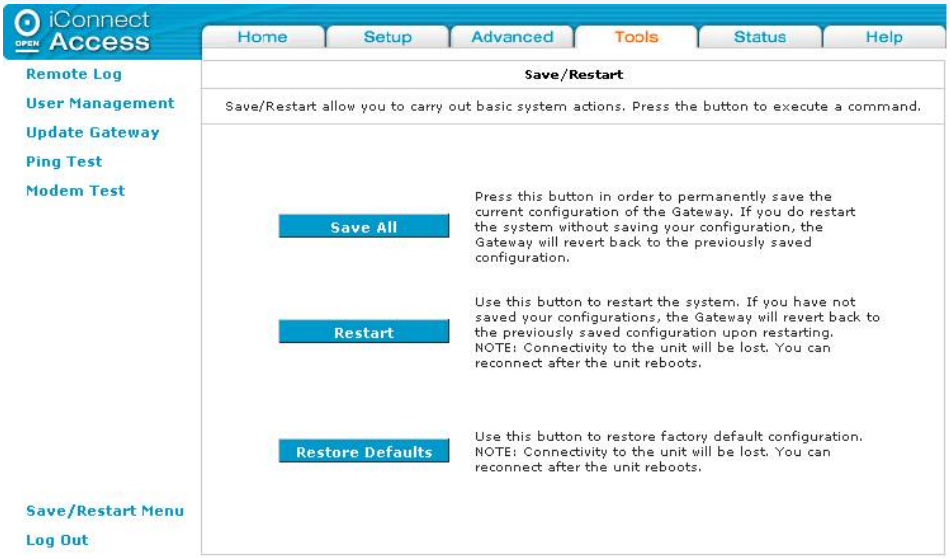
It is recommended that Static IP Addresses rather than DHCP IP Addresses be used for Port Forwarding.

---

step 6 In the *Category* area of the screen, highlight the appropriate category radio button. The *Available Rules* area displays common Internet services within the selected category. Rules for each service can be viewed by clicking the **View** button.

step 7 To add a rule for this connection, highlight the service / application from the *Available Rules* window, then click **Add**.
The rule then appears in the *Applied Rules* area of the screen.

step 8 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

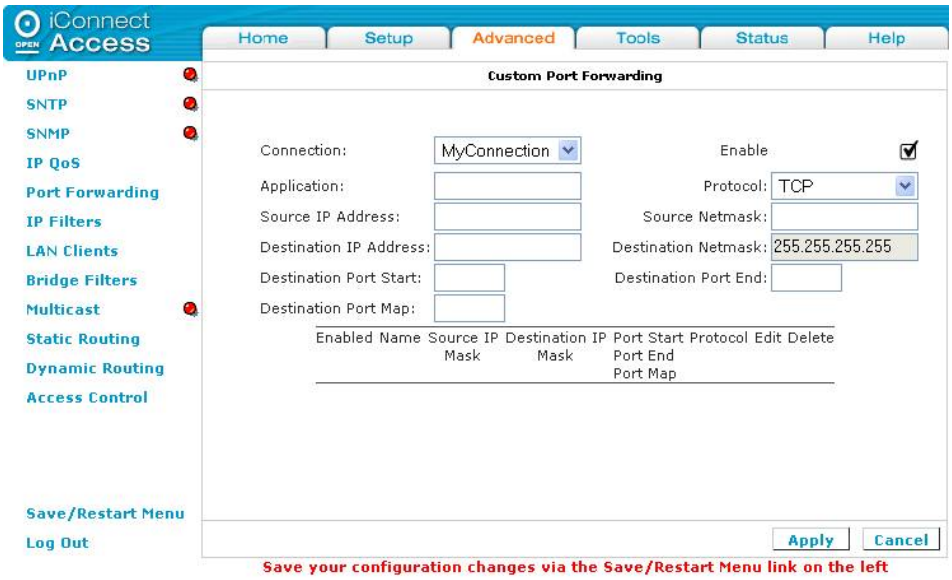
step 9 Click **Save All** to save the changes permanently.

The following table lists the *Port Forwarding* screen fields and their definitions:

Field	Description
WAN Connection	This is the list of connections defined in the *WAN Setup* area of the interface.
Select LAN Group	Select the LAN Group that contains the IP Host on which you wish to enable Port Forwarding from the drop-down list.
Allow Incoming Ping	Ping is a protocol used mainly for monitoring the connectivity between IP devices. Enabling this feature allows remote devices to use Ping to check connectivity to your device. You may need to enable this for monitoring purposes.
LAN IP	This is the server IP address to which the selected Ports are forwarded. It is recommended that you use a static IP address for Server. You will need to define this in the LAN Clients screen. See *To Add A LAN Client:*
Category/Available Rules	A number of pre-defined categories and rules are available here. E.g.: Web servers specifies the following port forwarding profile: **Rule Management** Rule Name: Web Server Cancel Protocol / Port Start / Port End / Port Map TCP 80 80 80 TCP 443 443 443 To view the details of a pre-defined rule, click **View**.
Applied Rules	This specifies the applied Port Forwarding rule for the selected WAN Connection and the LAN IP.
Custom Rules	You can specify custom Port Forwarding rules by clicking the **Custom Port Forwarding** link.

Custom Port Forwarding

step 1 From the *Port Forwarding* screen, click **Custom Port Forwarding** to define Port Forwarding rules. The following screen appears:



step 2 From the Connection: drop-down list, select the connection name for which you wish to set up port forwarding rules.

step 3 Enter a unique name for the rule in the *Application* field.

step 4 Identify the traffic by source and destination address and ports.

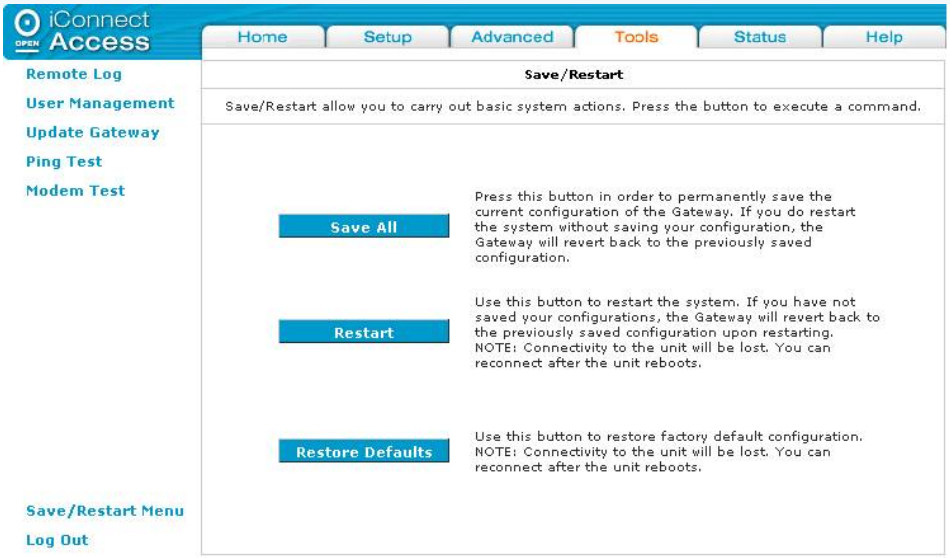
Use the IP Address 0.0.0.0 with a netmask of 0.0.0.0 in the Source Address if your IP Address is dynamically-assigned.

step 5 Select the protocol from the *Protocol* drop-down list. The options are: *TCP, UDP, ICMP* or *ANY*.

step 6 Enter the Destination IP Address and Netmask of the server to which the traffic is being forwarded.

step 7 Enter the destination port map on which the server will respond, in the *Destination Port Map* field.

step 8 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 9 Click **Save All** to save the changes permanently.

The following table lists the *Custom Port Forwarding* screen fields and their definitions:

Field	Description
Connection	Select the name of the connection for which you wish to customise Port Forwarding.
Enable	Check this checkbox to enable the customisation.
Protocol	Select the protocol. The options are: *TCP, UDP, ICMP* or *ANY*.
Application	Enter a unique name for the rule in this field.
Source IP	The IP address of the WAN interface to be forwarded, or 0.0.0.0 if the address is dynamically-assigned.
Source Netmask	The Network Mask of the WAN interface to be forwarded, or 0.0.0.0 if the address is dynamically-assigned.
Destination IP	The IP address of the device that is the receiving the traffic.
Destination Netmask	The Network Mask of the device that is receiving the traffic.
Destination Start Port *Destination End Port*	The port number/port range between which the traffic will arrive at the iConnectAccess624 WAN interface. The port range must be between 1 – 65535.
Destination Port Map	The port number on the LAN that is to receive the traffic.

Enable Incoming ICMP Ping

Enabling the Incoming Internet Control Message Protocol (ICMP) Ping will allow Echo requests to come into the gateway. The gateway will respond with an ICMP Echo response message. The option allows the DSL provider or ISP to determine the following:

- The status of the network;
- Tracking and isolating hardware and software problems;
- Testing, measuring, and managing networks.

Access Control

The iConnectAccess624's Access Control management feature opens access from the Internet (WAN) or (LAN) to the router's management ports (Web, Telnet, SSH, FTP, TFTP, SNMP). Note that there are security risks associated with this action, and for this reason, remote management is restricted to computers on the network that are specified in the IP Access Control List. (This holds up to 16 IP Addresses.)

The Access Control List (ACL) provides a global enable / disable. If the ACL is disabled, the default behaviour (ie, Deny for WAN, and Accept for LAN, is enabled for all IP addresses) is enforced. If no IP Addresses are specified in the ACL, the ACL will act as if it is disabled until the first IP Address is added.

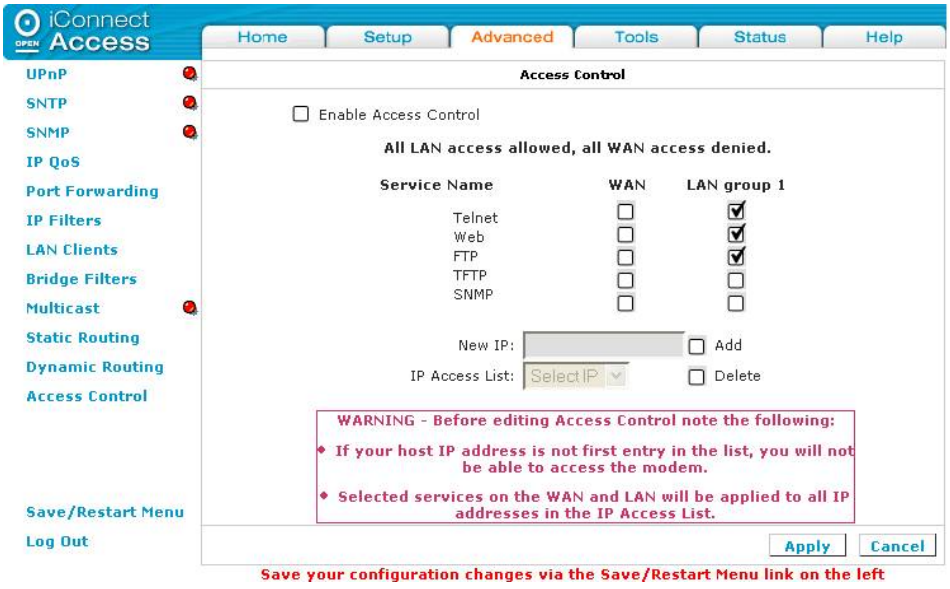
NOTE:

You must ensure that you add your own IP Address to the IP Access List, otherwise you could lock yourself out of the router. Should this occur and the setting is saved, you will need to perform a factory default reset, using the reset button.

To Enable Access Control:

From any screen in the web interface,

step 1 Click **Advanced**, then click **Access Control.** The following appears:



step 2 Check the *Enable Access Control* checkbox.

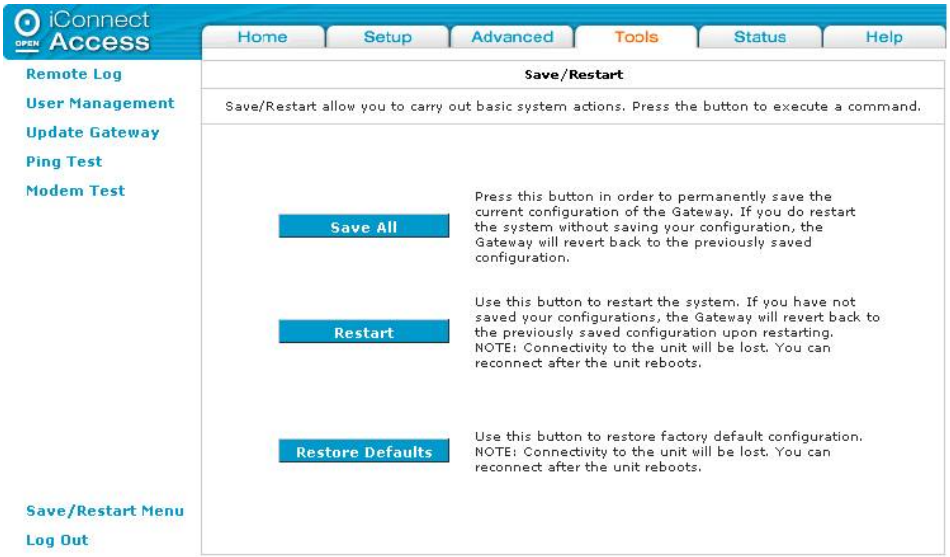
step 3 Check the services you wish to enable on the LAN and WAN sides.

step 4 To allow all IP Addresses, highlight the *Allow All* radio button. If you wish to allow a single IP Address in the Access Control List, highlight the *Select IP*

Address field for which services on the WAN and LAN sides are to be allowed. If you wish to enter a range of IP Addresses in the Access Control List, enter the start and end IP Addresses in the *Start IP Address* and *End IP Address* fields.

step 5 Check the **Add** checkbox.

step 6 Click **Apply** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 7 Click **Save All** to save the changes permanently.

The following table lists the *Access Control* screen fields and their definitions:

Field	Description
Enable Access Control	Global Enable / Disable that enables or disables the ACL.
Service Name (WAN / LAN)	Services that can be opened on the LAN and WAN sides of the iConnectAccess624. The options are: *Telnet, Web, FTP, TFTP, SNMP*. Select as many as required.
IP Access List	List of allowed IP Addresses.
New IP Address	Specify the new management host IP Address.
Add	Once you have specified the new management host IP Address, check the *Add* checkbox to add it.
Delete	Highlight the existing host IP Address and check the *Delete* checkbox.

DMZ Configuration

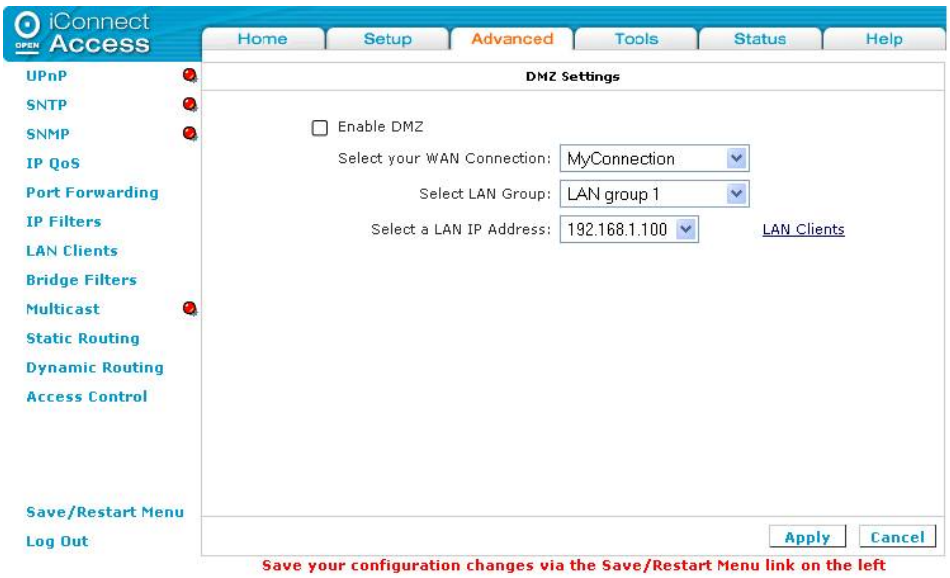
Setting a computer (on your local network) as a De-Militarised Zone (DMZ) forwards any network traffic that is not redirected to another computer via the port-forwarding feature to the computer's IP address. This opens access to the DMZ computer from the Internet.

To Configure A DMZ:

From any screen in the web interface,

step 1 Click **Advanced**, then click **Port Forwarding.**

step 2 From the *Port Forwarding* screen, click the **DMZ** link. The following appears:



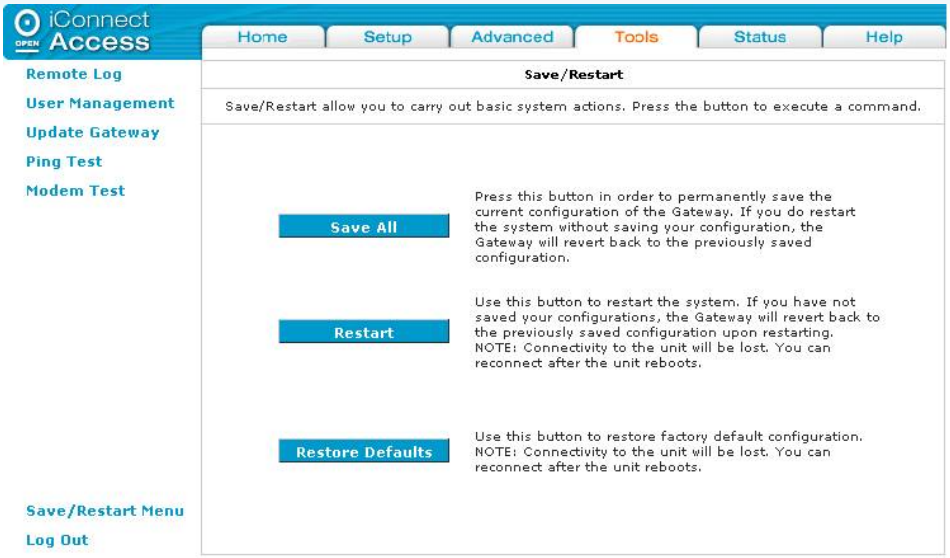
step 3 Check the *Enable DMZ* checkbox.

step 4 From the *Select your WAN Connection* drop-down list, select the connection type for which you wish to add the DMZ.

step 5 From the *Select LAN Group:* drop-down list, select the LAN group for which you wish to enable the DMZ.

step 6 Select the DMZ Host IP Address from the *Select a LAN IP Address* drop-down list. If your IP Address is not listed, click **LAN Clients**, and follow instructions in To Add A LAN Client:.

step 7 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 8 Click **Save All** to save the changes permanently.

The following table lists the *DMZ Settings* screen fields and their definitions:

Field	Description
Enable DMZ	Enables / Disables DMZ feature.
Select your WAN Connection	List of connections defined in the WAN Setup.
Select LAN Group:	Select the LAN Group for which you wish to enable the DMZ from the drop-down list.
Select a LAN IP Address	Host computer to act as the DMZ.

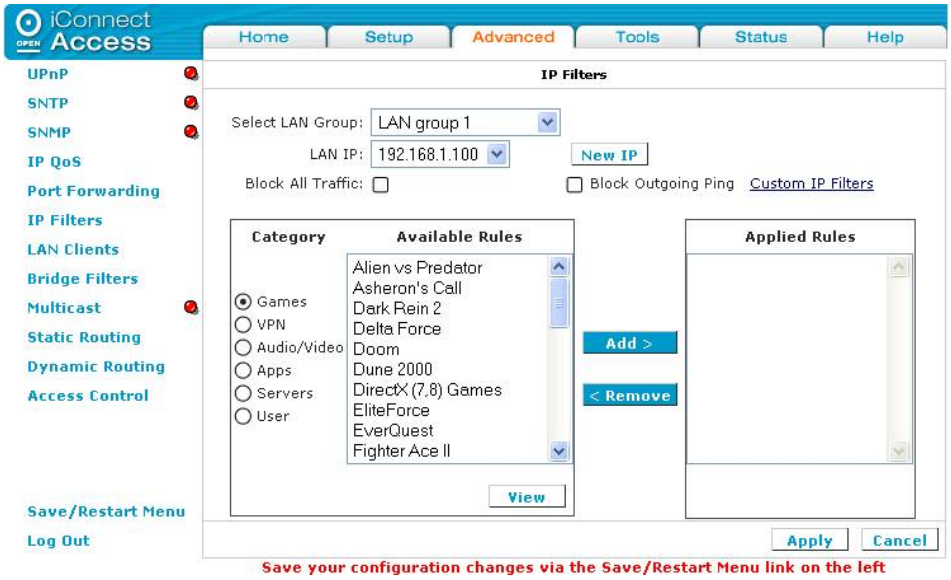
IP Filters

IP Filters allow you to block network access based on a user's computer IP Address on the local LAN. You can use this option to block specific traffic (eg, to block web access) or any traffic from a computer on your local network. If the traffic type is set to *Any*, all network traffic from that computer will be blocked. You can also add / edit / delete IP Filter rules without using the pre-defined rules. Click **Custom IP Filters** to access this interface.

To Configure IP Filtering:

From any screen in the web interface,

step 1 Click **Advanced,** then **IP Filters**. The following appears:



step 2 From the *LAN IP* drop-down list, select the IP Address for which you wish to apply the rule. If your IP address is not listed, click the **New IP** button, and following the instructions in To Add A LAN Client:.

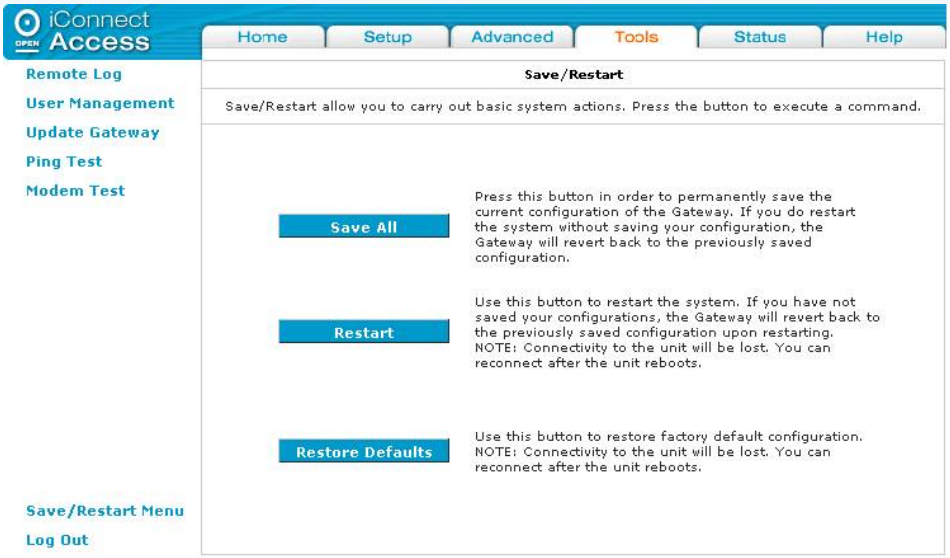
NOTE:

It is recommended that Static IP Addresses rather than DHCP IP Addresses be used for IP Filtering.

step 3 In the *Category* area of the screen, highlight the appropriate radio button for the category. The *Available Rules* area displays common Internet services within the category selected. Rules for each service can be viewed by clicking the **View** button.

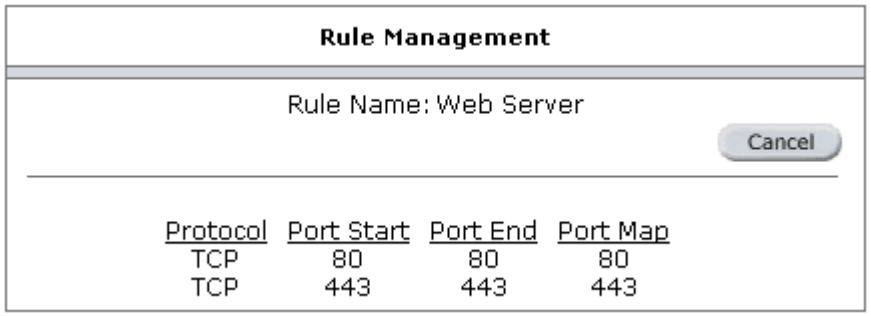
step 4 To add a rule for this connection, highlight the service or application from the *Available Rules* window, then click **Add**. The rule then appears in the *Applied Rules* area of the screen.

step 5 Click **Apply,** then click **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 6 Click **Save All** to save the changes permanently.

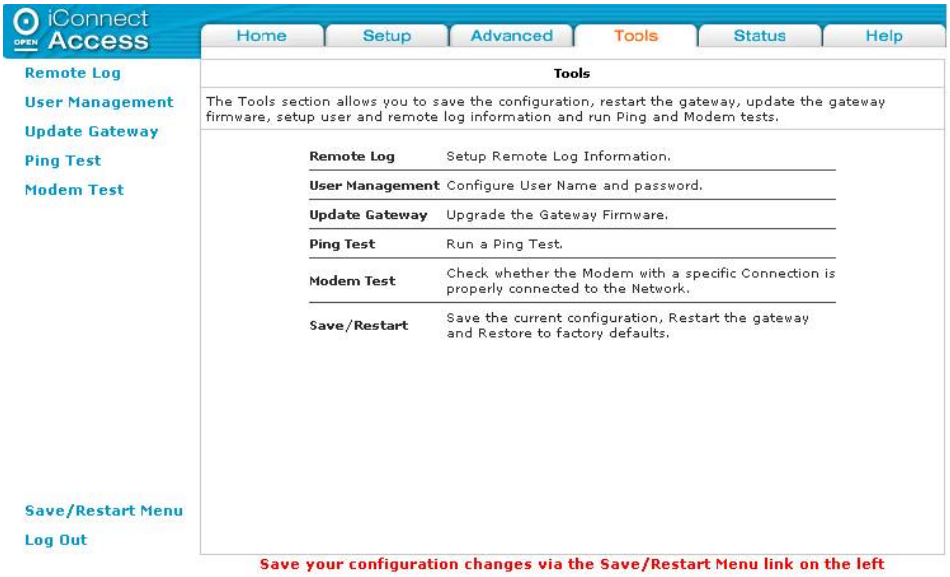
The following table lists the *IP Filtering* screen fields and their definitions:

Field	Description
Select LAN Group	Select a LAN (as specified in the *LAN Configuration* screen) from the drop-down list.
LAN IP	This is the server IP address to which Ports are forwarded. It is recommended that you use a static IP address for Server. This address will need to be defined in the LAN Clients screen. See *To Add A LAN Client:*
Block All Traffic	This option blocks all IP traffic from the specified LAN IP Address.
Block Outgoing Ping	This option blocks ICMP traffic from the specified LAN IP Address.
Category/Available Rules	A number of pre-defined categories and rules are available here. E.g.: Web servers specifies the following port forwarding profile:  To view the details of a pre-defined rule, click **View**.
Applied Rules	This specifies the applied IP filtering rule for the selected LAN IP Address.
Custom Rules	You can specify custom IP Filtering rules by clicking the **Custom IP Filters** button.

Tools

The Tools tab of the iConnectAccess624 web interface allows you to customise and debug your iConnectAccess624, update the firmware and perform network diagnostics. Its options include:

- Remote Log;
- User Management;
- Update Firmware;
- Ping Test;
- Modem Test;
- Save / Restart


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart Menu
Log Out
Tools
The Tools section allows you to save the configuration, restart the gateway, update the gateway firmware, setup user and remote log information and run Ping and Modem tests.
Remote Log
Setup Remote Log Information.
User Management
Configure User Name and password.
Update Gateway
Upgrade the Gateway Firmware.
Ping Test
Run a Ping Test.
Modem Test
Check whether the Modem with a specific Connection is properly connected to the Network.
Save/Restart
Save the current configuration, Restart the gateway and Restore to factory defaults.
Save your configuration changes via the Save/Restart Menu link on the left

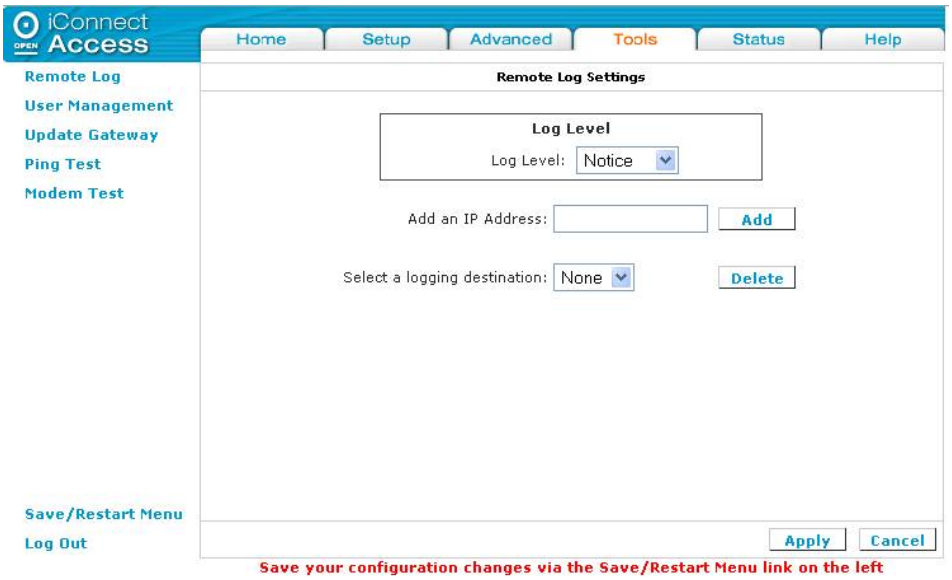
Remote Log

Remote Log enables logging in information to be sent to an external Syslog server. This allows for logging information to be retained for an extended period, depending on the capacity of the Syslog server.

When selecting a logging level, *Panic* will log only major events, where *Info* will log all events from *Panic* to *Info.*

From any screen in the web interface,

step 1 Click **Tools**, then **Remote Log**. The following screen appears:

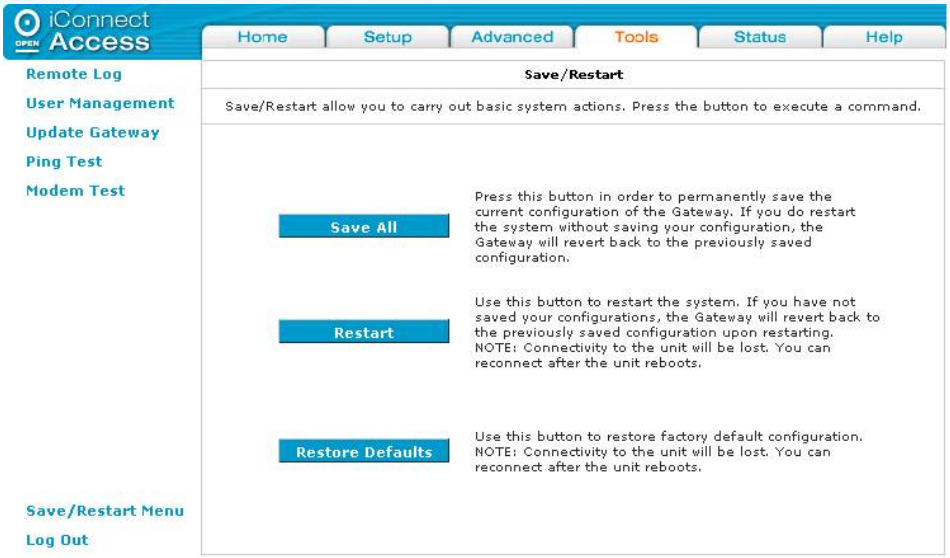


step 2 From the *Log Level* drop-down list, select the category at which a remote log is activated. The options are: *Panic*, *Alert, Critical, Error, Warning Notice, Information* or *Debug*.

step 3 Enter the IP address to which the log will be sent in the *Add an IP Address:* field, then click **Add**.

step 4 From the *Select a logging destination:* drop-down list, select the IP address of the logging destination.

step 5 Click **Apply,** then **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 6 Click **Save All** to save the changes permanently.

The following table lists the *Remote Log Settings* screen fields and their definitions:

Field	Description
Log Level	Select the level of logging required. The selected option will include the following: *Panic*, *Alert, Critical, Error, Warning Notice, Information* or *Debug*.
Add an IP Address	The Syslog Server IP Address.
Select a logging destination	When an IP Address is added it appears in this field. Select the IP Address to change level or remove.

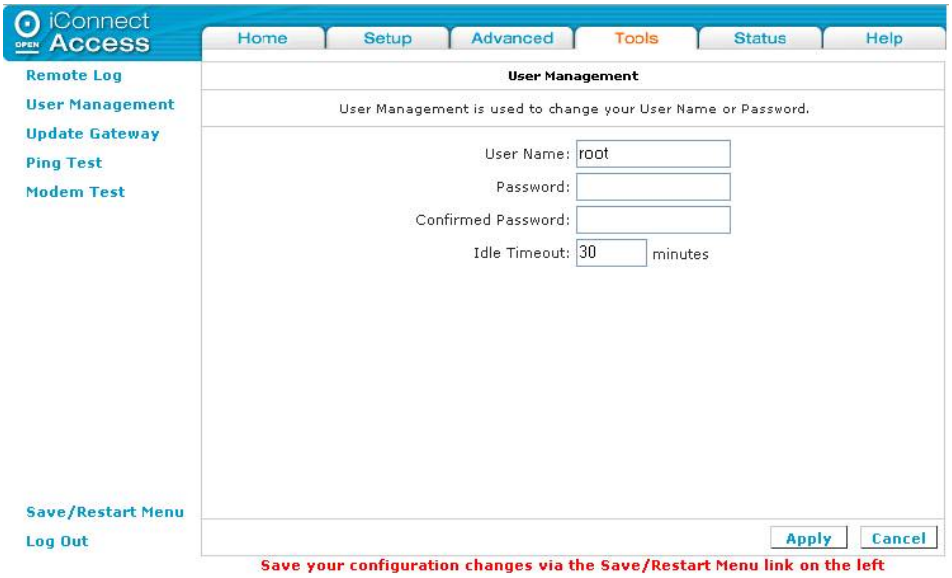
User Management

You can change your iConnectAccess624's username and password by clicking User Management from the Tools menu list. From here you can change the login name and password. You can also change the idle timeout; you will need to log back onto the iConnectAccess624 once the timeout expires.

To Change The iConnectAccess624 Password:

From any screen in the web interface,

step 1 Click **Tools**, then **User Management** from the menu list. The following screen appears:



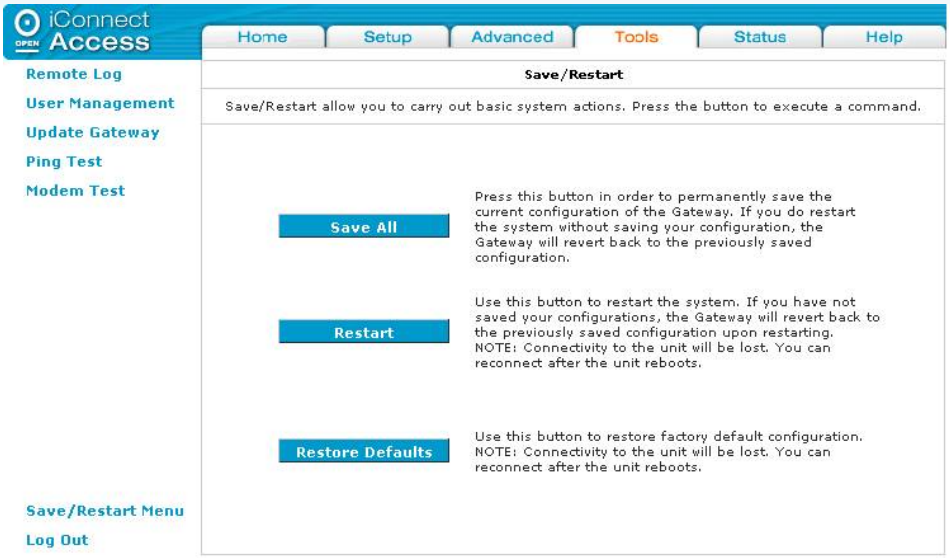
step 2 Enter a user name for the root user in the *User Name* field.

step 3 Enter a password for the root user in the *Password* field.

step 4 Confirm the password by re-typing it in the *Confirmed Password* field.

step 5 If you wish to change the idle timeout, enter a new timeout in minutes in the *Idle Timeout* field.

step 6 Click **Apply,** then **Save / Restart Menu.** The following appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration. NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

step 7 Click **Save All** to make the changes permanent.

NOTE:

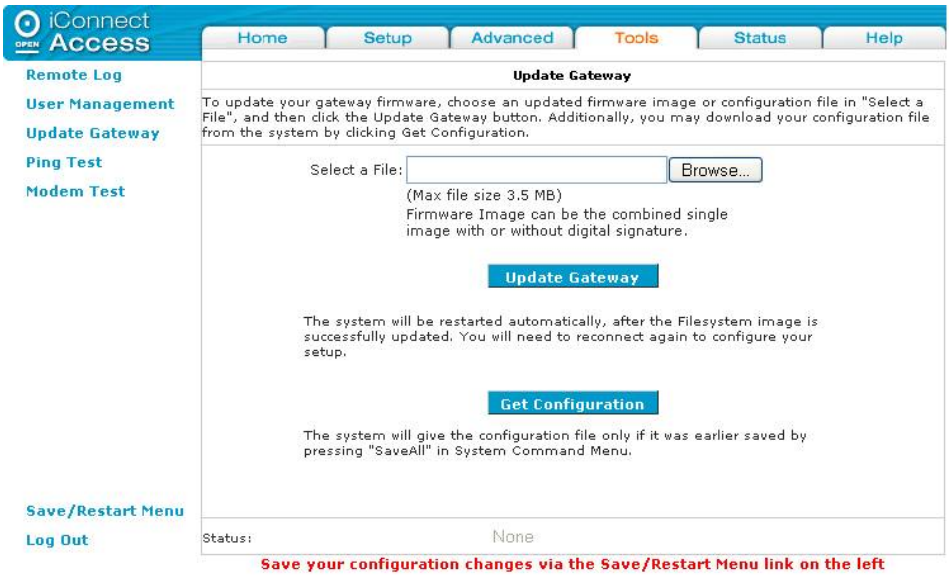
If you forget your password, press and hold the reset to factory defaults button for 10 seconds (or more). The iConnectAccess624 will reset to its factory default configuration and all customised configurations will be lost.

Update Gateway

To Upgrade The iConnectAccess624 Firmware:

From any screen in the web interface,

step 1 Click **Tools**, then **Update Gateway** from the menu list. The following screen appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Update Gateway
To update your gateway firmware, choose an updated firmware image or configuration file in "Select a File", and then click the Update Gateway button. Additionally, you may download your configuration file from the system by clicking Get Configuration.
Select a File:
Browse...
(Max file size 3.5 MB)
Firmware Image can be the combined single image with or without digital signature.
Update Gateway
The system will be restarted automatically, after the Filesystem image is successfully updated. You will need to reconnect again to configure your setup.
Get Configuration
The system will give the configuration file only if it was earlier saved by pressing "SaveAll" in System Command Menu.
Save/Restart Menu
Log Out
Status:
None
Save your configuration changes via the Save/Restart Menu link on the left

step 2 In the *Update Gateway* screen, click the **Browse** button beside the *Select A File* field to search for the new firmware. Ensure the upgrade file is in **.img* format.

step 3 In the *Choose File* window, select the file and click **Open**.

step 4 Click **Update Gateway**.

NOTE:

The firmware upgrade should take around five minutes to complete. Once complete, the iConnectAccess624 will reboot, and you will then need to log back into it. Do not remove power from the iConnectAccess624 during the firmware upgrade procedure.

Ping Test

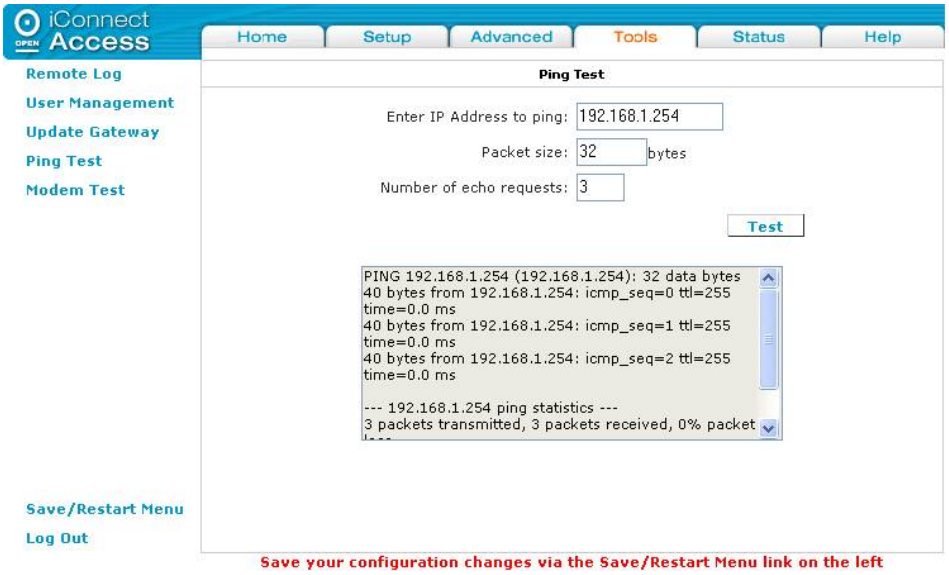
Ping is a diagnostic tool used to test connectivity between IP Hosts. When a Ping test is conducted, a small amount of data is sent from one computer to another and back again, and the time it takes is reported in milliseconds. This can be used on a LAN or across the Internet.

Once you have configured your iConnectAccess624, it is a good idea to ensure you can Ping a network device. If your ISP has provided its gateway address, you can try to ping this address. If the Pings for both the WAN and LAN side complete and you have the proper protocols configured, you will be able to surf the Internet.

To Perform A Ping Test:

From any screen in the web interface,

step 1 Click the **Tools** tab, then click **Ping Test**. The following screen appears:



step 2 Enter the target address to be pinged in the *Enter IP Address to ping* field.

step 3 In the *Packet size* field, enter the required packet size or leave at the default.

step 4 In the *Number of echo requests* field, enter the number of echo requests, then click **Test**. The iConnectAccess624 will ping the specified address, and you will be able to see the results in the display area beneath the Test button.

The following table lists the *Ping Test* screen fields and their definitions:

Field	Description
Enter IP address to ping	This is the IP address of the destination device that you want to ping. If the ping is successful, it means that the iConnectAccess624 has IP connectivity to this device.
Packet size	The packet size can be defined for the Ping request.
Number of echo requests	The number of ping packets that you want to send in the sequence.

Modem Test

The Modem Test menu item allows you to check whether your iConnectAccess624 is properly connected to the WAN Network. There are four test types, each of which may take a few seconds to complete.

The OAM loopback cells are used to verify the connection between the iConnectAccess624 and the ATM network. For the iConnectAccess624, OAM loopback provides a valuable tool for diagnosing problems with the DSL line.

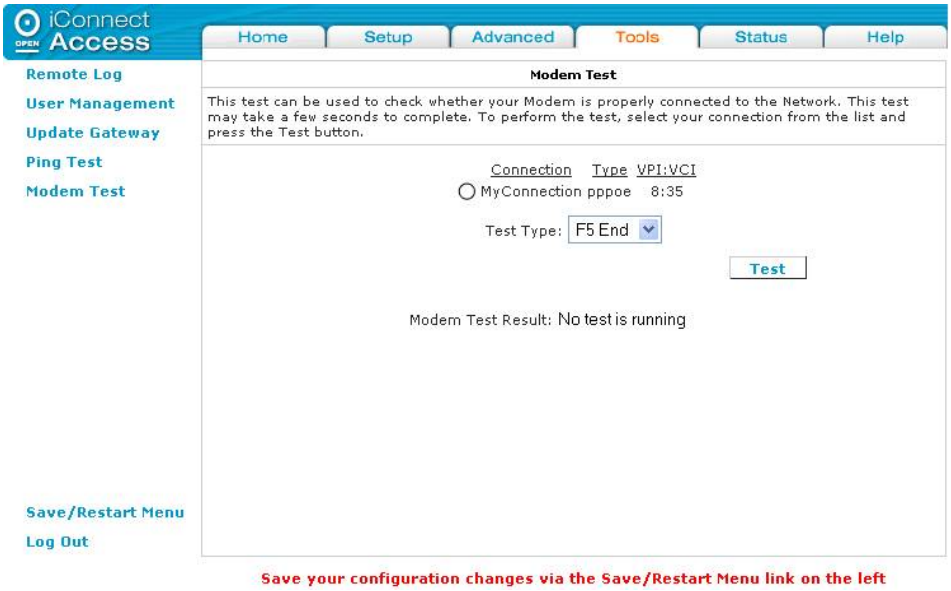
Before you attempt any of these modem tests, ensure the following:

- Your DSL Provider / ISP supports them;
- You have a valid DSL link.

To Perform A Modem Test:

From any screen in the web interface,

step 1 Click the **Tools** tab, then click **Modem Test**. The following screen appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart Menu
Log Out
Modem Test
This test can be used to check whether your Modem is properly connected to the Network. This test may take a few seconds to complete. To perform the test, select your connection from the list and press the Test button.
Connection Type VPI:VCI
MyConnection pppoe 8:35
Test Type: F5 End
Test
Modem Test Result: No test is running
Save your configuration changes via the Save/Restart Menu link on the left

step 2 Select your connection from the list.

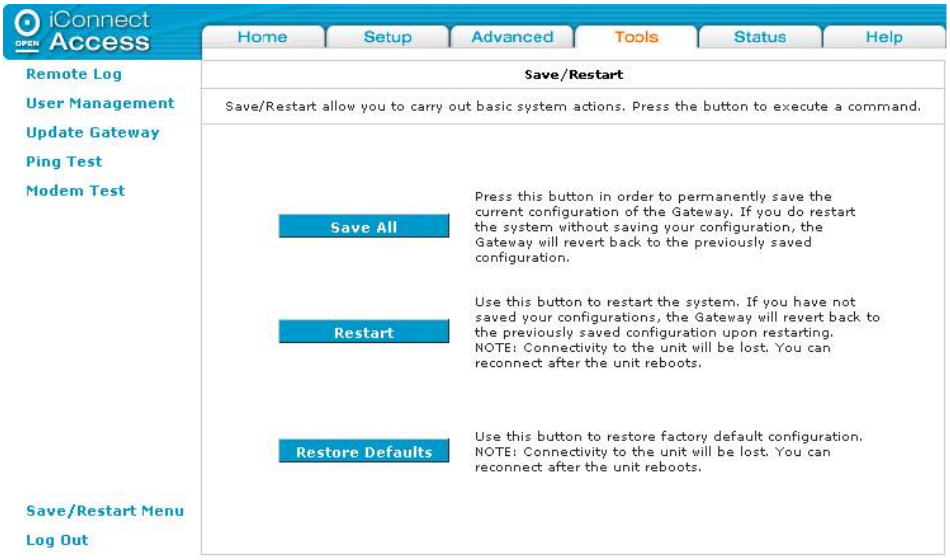
step 3 Select the type of test to perform from the *Test Type* drop-down list, then click **Test**.

The following table lists the *Modem Test* screen Test Type field and its definitions:

Field	Options	Description
Test Type	*F5 End*	Connectivity to the BRAS server can be verified by initiating a F5 Seg loopback via the DSLAM and to the authentication server.
	F5 Seg	Lost and corrupted ATM cells can be quickly ruled out in the field by initiating a F5 Seg loopback (also known as ATM ping) to the DSLAM and have the DSLAM respond by looping back the OAM cells. By ruling out problems with the ATM Layer, the service provider can then focus on examining higher layer protocols and other configurations to isolate the problem.
	F4 End and F4 Seg Tests	You can perform two types of OAM F4 Tests: *Segment*—the end of a connection segment *End-to-end*—the end of a VC/VP connection where the ATM cells are terminated

Save / Restart Menu

To make changes permanent on the web interface you need to click the **Save / Restart Menu** link from the menu list. The following commands are used to configure the iConnectAccess624:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Remote Log
User Management
Update Gateway
Ping Test
Modem Test
Save/Restart
Save/Restart allow you to carry out basic system actions. Press the button to execute a command.
Save All
Press this button in order to permanently save the current configuration of the Gateway. If you do restart the system without saving your configuration, the Gateway will revert back to the previously saved configuration.
Restart
Use this button to restart the system. If you have not saved your configurations, the Gateway will revert back to the previously saved configuration upon restarting.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Restore Defaults
Use this button to restore factory default configuration.
NOTE: Connectivity to the unit will be lost. You can reconnect after the unit reboots.
Save/Restart Menu
Log Out

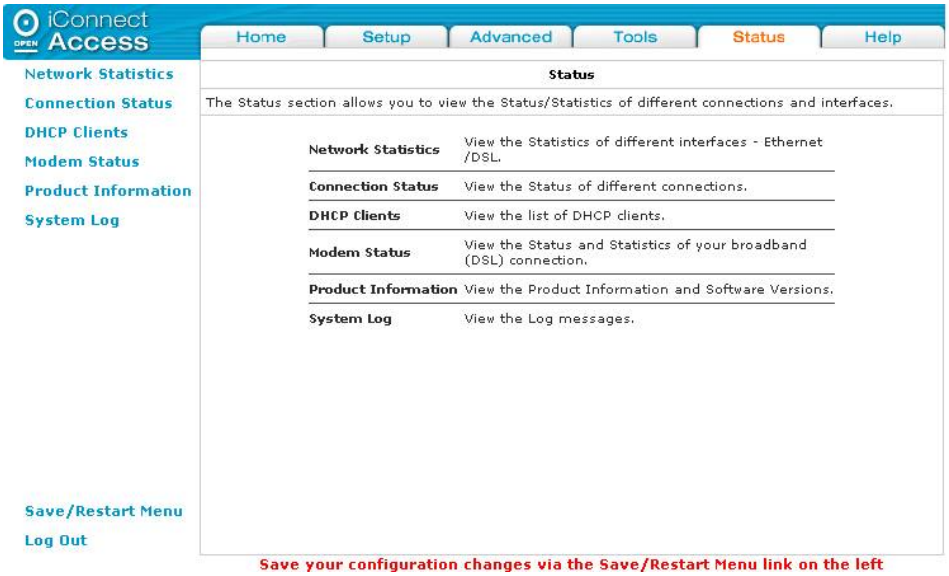
The following table lists the *Save / Restart* screen buttons and their definitions:

Field	Description
Save All	Click this button to save the current configuration of the iConnectAccess624 permanently. If you do restart the system without saving your configuration, the iConnectAccess624 will revert back to the previously saved configuration.
Restart	Click this button to re-start the system. If you have not saved your configurations, the iConnectAccess624 will revert back to the previously saved configuration upon re-starting. *NOTE:* *Connectivity to the unit will be lost. You can reconnect after the unit reboots.*
Restore Defaults	Click this button to restore the factory default configuration. *NOTE:* *Connectivity to the unit and all configuration will be lost. You can reconnect after the unit reboots.*

Status

The Status tab of the iConnectAccess624 web interface allows you to view the Status/Statistics of different connections and interfaces, and consists of the following:

- Network Statistics;
- Connection Status;
- DHCP Clients;
- Modem Status;
- Product Information;
- System Log.



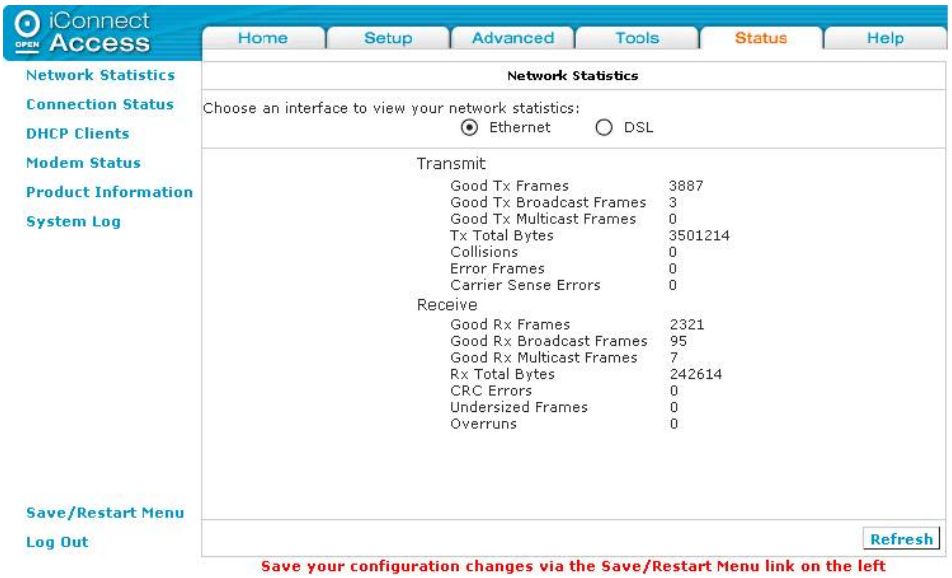
Network Statistics

The Network Statistics area will show you details of transmitted and received packets.

To View Network Statistics:

From any screen in the web interface,

- Click the **Status** tab, then click **Network Statistics**. A screen with details similar to those below appears:



- In the *Network Statistics* screen, highlight the appropriate radio button corresponding to view network statistics for *Ethernet* or *DSL*. Click **Refresh**.

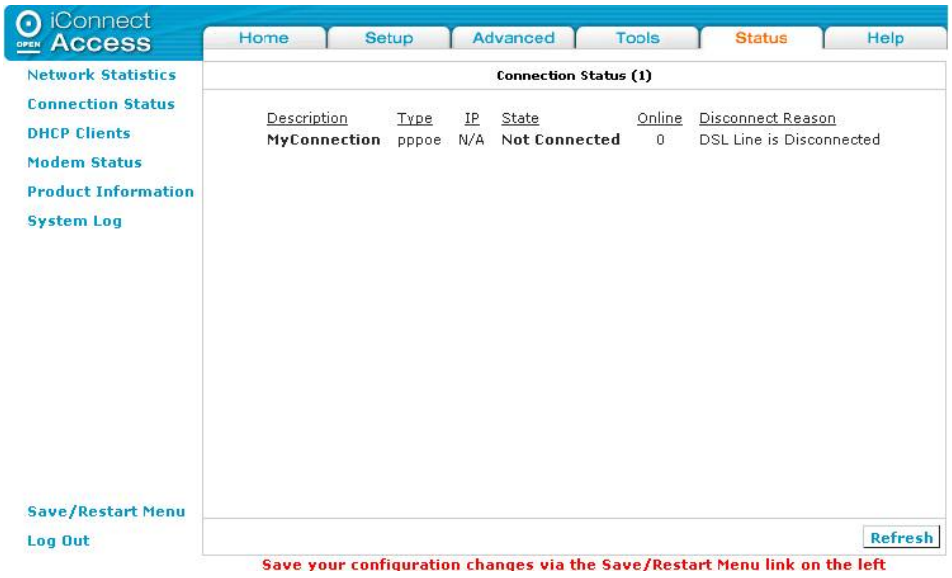
Connection Status

The *Connection Status* screen displays a status summary of the ADSL connection.

To View Connection Status:

From any screen in the web interface,

- Click the **Status** tab, then click **Connection Status**. A screen with details similar to those below appears:



- Click **Refresh** when you wish to update the details on the screen.

The following table lists the *Connections* screen fields and their definitions:

Field	Description
Description	This is the name of the connected ADSL profile.
Type	Authentication type of the ADSL connection is listed here. E.g.: PPPoE, PPPoA, Static etc:
IP	The WAN IP Address is displayed here when the connection is established.
State	ADSL connection status is displayed here. This is the connection between your iConnectAccess624 and the DSLAM at your ISP. In normal operation, this must be connected.
Online	The duration of the Internet connection time for the Connection type specified.
Disconnect Reason	If the connection is not active, the reason for disconnection is displayed here.

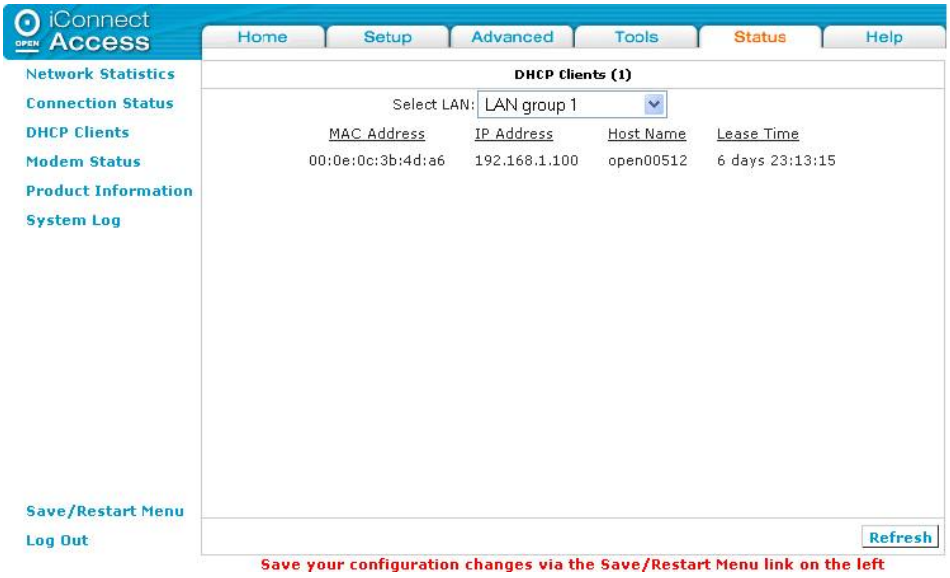
DHCP Clients

Select the **DHCP Clients** menu item from the *Status* menu list to view the list of DHCP clients on your LAN.

To View DHCP Clients:

From any screen in the web interface,

- Click the **Status** tab, then click **DHCP Clients**.
  A screen with similar details to those shown below appears:



- From the *Select LAN* drop-down list, select the LAN computer whose DHCP details you wish to view.
- Click **Refresh** when you wish to update the details on the screen.

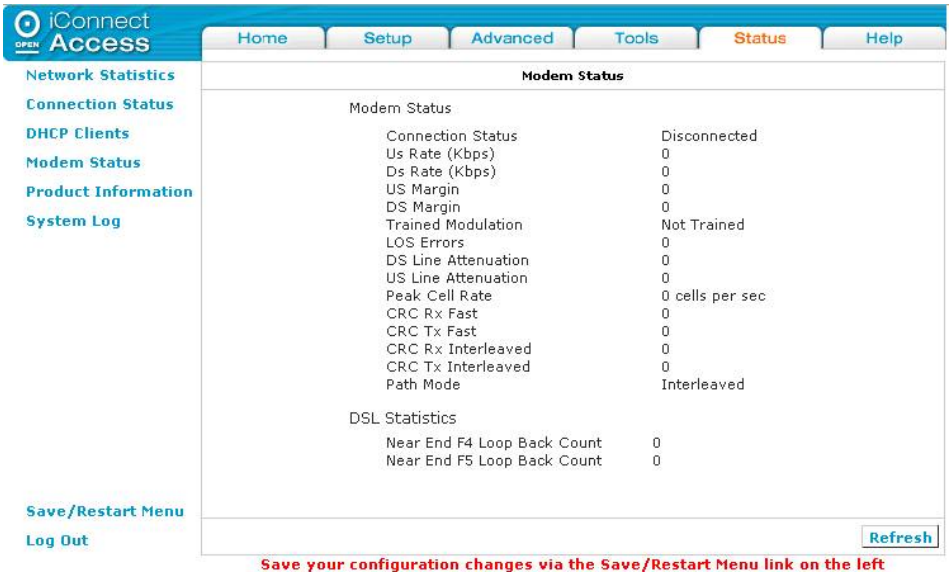
Modem Status

Select the **Modem Status** menu item from the *Status* menu list to view the Status and Statistics of your broadband (DSL) connection.

To View The Modem Status:

From any screen in the web interface,

- Click the **Status** tab, then click **Modem Status**. A screen with details similar to those below appears:



- Click **Refresh** when you wish to update the details on the screen.

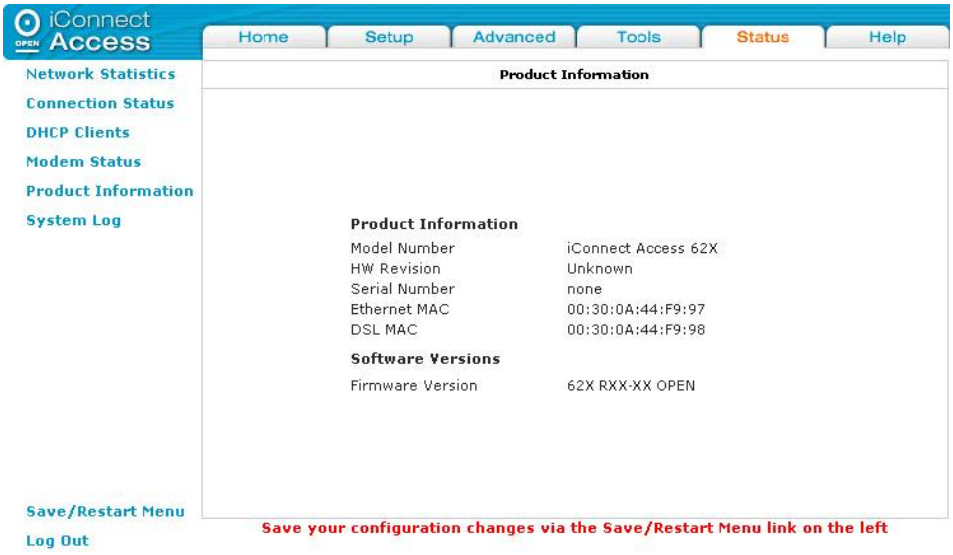
Product Information

You can verify product information such as model, driver, hardware and software versions in the *Product Information* area of the web interface.

To View iConnectAccess624 Product Information:

From any screen in the web interface,

- Click the **Status** tab, then click **Product Information**. A screen with details similar to those below appears:



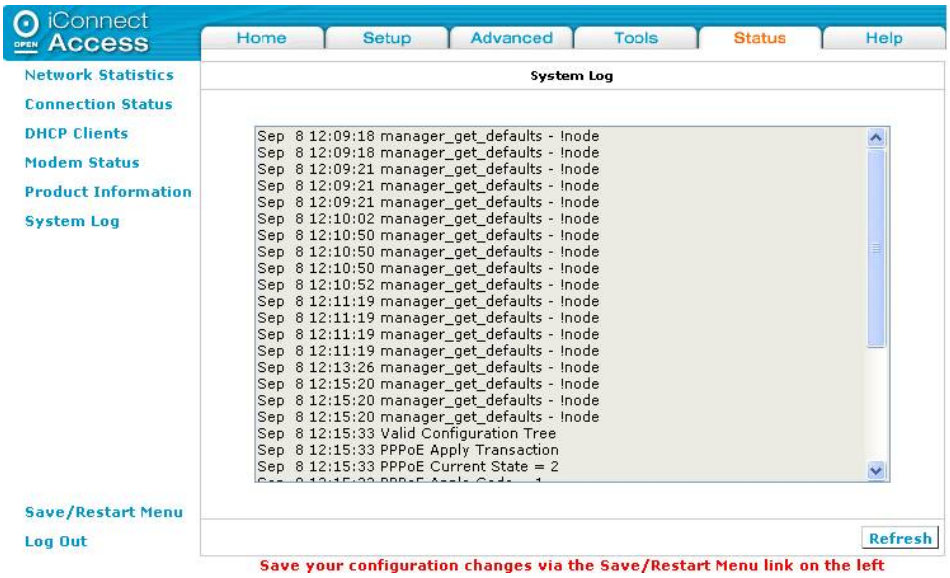
System Log

You can view all logged information in the System Log area of the web interface.

To Display The iConnectAccess624 System Log:

From any screen in the web interface,

- Click the **Status** tab, then click **System Log**. A screen with details similar to those below appears:


iConnect Access
Home
Setup
Advanced
Tools
Status
Help
Network Statistics
Connection Status
DHCP Clients
Modem Status
Product Information
System Log
Save/Restart Menu
Log Out
System Log
Sep 8 12:09:18 manager_get_defaults - Inode
Sep 8 12:09:18 manager_get_defaults - Inode
Sep 8 12:09:21 manager_get_defaults - Inode
Sep 8 12:09:21 manager_get_defaults - Inode
Sep 8 12:09:21 manager_get_defaults - Inode
Sep 8 12:10:02 manager_get_defaults - Inode
Sep 8 12:10:50 manager_get_defaults - Inode
Sep 8 12:10:50 manager_get_defaults - Inode
Sep 8 12:10:50 manager_get_defaults - Inode
Sep 8 12:10:52 manager_get_defaults - Inode
Sep 8 12:11:19 manager_get_defaults - Inode
Sep 8 12:11:19 manager_get_defaults - Inode
Sep 8 12:11:19 manager_get_defaults - Inode
Sep 8 12:11:19 manager_get_defaults - Inode
Sep 8 12:13:26 manager_get_defaults - Inode
Sep 8 12:15:20 manager_get_defaults - Inode
Sep 8 12:15:20 manager_get_defaults - Inode
Sep 8 12:15:20 manager_get_defaults - Inode
Sep 8 12:15:33 Valid Configuration Tree
Sep 8 12:15:33 PPPoE Apply Transaction
Sep 8 12:15:33 PPPoE Current State = 2
Refresh
Save your configuration changes via the Save/Restart Menu link on the left

- Click **Refresh** when you wish to update the details on the screen.

Index

624 Ports And Buttons
DC, 8
Ethernet, 8
Reset, 8
Advanced Security Features
Incoming ICMP Ping, 69
Advanced Tab, 44
Bridge Filter Rules, Hidden, 57
Bridge Filters, 55
Dynamic Routing, Enabling, 62
Firewall, 64
IP QoS, Configuration Of, 50
LAN Clients, Adding, 54
Multicast, Enabling, 58
SNMP Configuration Of, 48
Static Routing, Enabling, 60
UPnP, 44
Ethernet Configuration
Windows 2000 / XP, 12
Windows 98 Second Edition / ME, 11
Firewall
Access Control, 69
DMZ, Configuration Of, 71
IP Filters, 73
Port Forwarding, 64
Front LED Panel, 10
Home Tab, 15
iConnectAccess624 Log In, 14
iConnectAccess624 Ports and Buttons, 8
iConnectAccess624 Ports And Buttons
ADSL, 8
iConnectAccess624, Installation Of, 11
iConnectAccess624, Setting Up, 13
LAN Configuration
Management IP Configuration, 21
LAN, Configuration Of, 17
Modem Set Up
ADSL Handshake, 42
Setting Up Your iConnectAccess624
Default Settings, 13
Status Tab, 85
Connection Status, 87
DHCP Clients, 88
Modem Status, 89
Network Statistics, 86
Product Information, 90
System Log, 91
Tools Tab, 75
Gateway Upgrade, 80
Modem Test, 82
Ping Test, 81
Save / Restart Menu, 84
User Management, 78
WAN Configuration
Bridged Connection Type, 31
Classical IP Over ATM (CLIP)
Connection, 40
Connection, Modification Of, 41
DHCP Connection, 37
PPPoA Connection, 28
PPPoE Connection, 25
Static Connection, 34
WAN, Configuration Of, 24